HARALD SEIZ

Wie GOLD unser Zahlungssystem revolutionieren wird

DIE ZUKUNFT DES GELDES

FBV

5.
Kriminalität, Krisen, Katastrophen – und die nötige Vorsorge

Eine Währung hat es nicht leicht: Sie ist nicht nur von den geldpolitischen Angelegenheiten abhängig, von der Wirtschaft und den Finanzmärkten, sondern sie ist auch der allgemeinen Weltlage ausgesetzt – und Kriminellen aller Art, auf die ich im folgenden Abschnitt zu sprechen komme. Dass Kriege, unkontrollierte Migrantenströme, Krisen und Anschläge uns nun auch vor unserer Haustür verunsichern, versteht sich von selbst. All dies verursacht millionenfaches Leid und wirft viele Menschen und Gesellschaften um Jahrzehnte zurück – natürlich auch die Volkswirtschaften und besonders die Infrastruktur. Wo Verunsicherung und Terror herrschen, baut sich niemand etwas auf. Unternehmerisches Denken sowie zukunftsfähige Investments fallen völlig aus, vom archaischen Kleinhandel und Durchwursteln einmal abgesehen.

Alle diese Zusammenhänge liegen auf der Hand. Doch gerade die Widrigkeiten und menschlichen Tragödien, die immer näher an uns heranrücken, zeigen einmal mehr die Notwendigkeit, sich auch bei uns auf alle Eventualitäten einzustellen, denn historisch gesehen ist unser Leben in Frieden leider eine Ausnahme. Dadurch haben wir es aber verlernt, uns auf Krisen einzustellen. Unsere Regierung kann weder eine verantwortliche und nachhalti-

ge Wirtschafts- und Sozialpolitik betreiben, noch kann sie offenbar ausreichend unser Leben und Zusammenleben schützen. Darauf müssen wir uns einstellen – nicht nur mit Vorräten, wie es selbst die Bundesregierung propagiert, sondern auch finanziell. Auch ich kann nicht in die Zukunft schauen, doch kann ich nur jedem raten, sich finanztechnisch gut vorzubereiten: mit dem richtigen Mix aus Bargeld, unterschiedlichen Stückelungen und Währungen, aber auch mit Realwerten, darunter Gold. Wir müssen uns auf einen Ausfall der elektronischen Banksysteme einstellen; sei es, weil es einen Hackerangriff gegeben hat oder kein Strom mehr da ist. Aber auch Versorgungsengpässe sind durchaus möglich. Wer da nicht nur 100 Liter Wasser und Konserven im Keller hat, sondern auch eine probate Mischung von Geld und Werten, mit der er sich gerade in der Not etwas kaufen kann, muss sich im Ernstfall nicht viel vorwerfen. Ich werde später verschiedene Möglichkeiten und Empfehlungen beschreiben, die die »Konzeption zivile Verteidigung« der Bundesregierung geldtechnisch ergänzen.

Wie sicher sind unsere Zahlungssysteme?

Es ist interessant, welche hohen Wellen es immer wieder schlägt, wenn jemand die Abschaffung des Bargeldes ins Spiel bringt. Denn das Bankenwesen – nicht unsere privaten Zahlungsvorgänge – ist längst ausschließlich elektronisch und digital organisiert. Rein technisch gesehen ist unser Geld bereits virtuell – und erscheint lediglich als 0 und 1 in den Computersystemen von Banken und Sparkassen. Entscheidend ist neben dem Wert, dass wir jederzeit an unser Erspartes herankommen. Schließlich ist es in der Regel eine der ersten staatlichen Maßnahmen, Geldabhebungen einzuschränken. In der Euro-Zone haben wir das 2013 in Zypern und 2015 in Griechenland erlebt, darüber habe ich im 2. Kapitel berichtet. In diesem Abschnitt soll es darum gehen, wie Cyber-Betrüger und Hacker versuchen, aus dem digitalen System Geld herauszuziehen.

Dabei geben sie sich nicht mehr mit ein paar 100.000 Euro ab, die man bei einem traditionellen Bankraub erbeutet. Die Summen, um die es hier geht, sind schwindelerregend. Dennoch ist privates Online-Banking in Deutschland sicher – erstaunlich angesichts der Vehemenz der Attacken: Sage und schreibe neun Millionen Angriffe durch Schadsoftware werden pro Monat auf deutsche Online-Banking-Plattformen ausgeführt. Fast alle davon werden abgewehrt, die Schäden betragen gerade einmal 0,01 Prozent des Transaktionsvolumens bei allen deutschen Instituten, berichtete Hans-Joachim Massenberg, Mitglied der Hauptgeschäftsführung des Bundesverbands deutscher Banken auf dem Zahlungsverkehrs-Symposium 2015 der Bundesbank: »Die Server der Banken, wie auch die Kommunikationskanäle von den Banken zum Kunden seien grundsätzlich sicher.«[146] Dies führe jedoch dazu, dass Kriminelle auf das schwächste Glied in der Kette der Online-Zahlungen umschwenken – den Kunden. Zudem befürchtet die Branche, dass das Aufkommen neuer Anbieter bei Online-Bezahlverfahren die Sicherheitsprobleme verschärft. Tatsächlich zeigt sich an den zahlreichen aufkommenden Bitcoin-Dienstleistern, wie junge Unternehmen neue Angriffsflächen bieten. Zudem sieht der Branchenvertreter Gefahren, wenn immer mehr Drittdienste Zugang zum Bankkonto erhalten – und dies nicht nur durch Hacken, sondern etwa durch Spammails, auf die die Nutzer reagieren.[147] Es liegt auf der Hand, dass zusätzliche Glieder in der Bezahlkette das Gesamtsystem schwächen – wobei langfristig andere Teile ersatzlos wegfallen könnten. Doch noch ist es nicht soweit und die Organisation der Zahlungsvorgänge weltweit wird durch neue Akteure verwundbarer.

Die Risiken der Digitalisierung

Attacken auf unsere lebenswichtige Infrastruktur sind keine Idee von Science-Fiction-Autoren oder Verschwörungstheoretikern. Je stärker unsere verschiedenen Lebensbereiche von Computern abhängig sind – und bald schon wird unser Kühlschrank dazugehö-

ren –, umso mehr Angriffsflächen bieten sie. Dabei ist das Beispiel aus dem Privathaushalt höchst real, denn dort beginnt oft die Arbeit der Kriminellen. Natürlich haben es Cyber-Terroristen in der Regel nicht darauf abgesehen, unser persönliches Umfeld auszuspähen oder uns gar Streiche zu spielen: Doch wie die 900.000 lahmgelegten Telekomrouter Ende 2016 gezeigt haben, werden die Geräte in unseren Haushalten in der Masse dafür genutzt, Attacken auf andere Systeme auszuführen, und zwar über ein Botnet, eine Gruppe von Schadprogrammen. Ziele der Aktionen sind existenzielle Einrichtungen: Stromversorger, Krankenhäuser, Wasserwerke, Fernsehsender und Banken. Sie werden mittels Hunderttausender von Rechnern, Routern und Geräten attackiert, sei es, weil die Verursacher damit eine politische Absicht verbinden, sei es, weil sie Chaos verursachen oder schlichtweg Geld rauben oder erpressen wollen.

Mit der zunehmenden – komfortablen und oft kostensparenden – Vernetzung unserer Länder, Geräte und Branchen werden die Systeme jedoch anfälliger für Cyber-Anschläge. Die Tatsache, dass das Internet ausdrücklich dezentral organisiert ist und es weltweit Hunderttausende verschiedene IT-Dienstleister gibt, bietet dabei keinerlei Schutz. Denn unterm Strich greifen sie alle nur auf eine Handvoll IT-Systeme, Softwareprogramme und auf eine überschaubare Anzahl von Speicherfarmen zurück. Damit wird der Nutzen eines dezentralen Netzes, das beim Ausfall eines einzelnen Elements weiterarbeiten kann – ein Grundprinzip des Internets und eines Netzes generell – in sein Gegenteil verkehrt. Erst Anfang März 2017 konnten wir diese Verwundbarkeit wieder erleben: Die Amazon-Tochter Amazon Web-Services (AWS) hatte massive Computerprobleme (wegen eines banalen Tippfehlers) und musste daraufhin neu gestartet werden. Doch nicht nur Amazon-Kunden schauten vier Stunden lang in die Röhre, sondern auch Nutzer von Expedia oder Snapchat, die auf diesen Cloud-Service von Amazon zurückgreifen.

Vor allem Stromversorger sind – neben Telekommunikationsgesellschaften und Banken – im Hinblick auf mögliche Attacken

besonders gefährdet: Laut F.A.Z. »warnen Fachleute vor Hackerangriffen speziell auf Unternehmen der Energiebranche. Die mangelhafte IT-Sicherheit bei den Versorgern sorge für ein steigendes Risiko von Stromausfällen. (...) Anders als gerne öffentlich behauptet, sind viele Energieversorger weiterhin ungenügend gegen Cyber-Attacken gewappnet«, wird dort Oliver Neumann zitiert, Sprecher der IT-Sicherheitsberatung Recurity Labs aus Berlin.[148]

Attacken auf Banken: Datenblackout und Cyber-Kriminalität

Bei den Banken sieht es nicht anders aus, wie zahlreiche digitale Banküberfälle der vergangenen Jahre zeigen. Laut F.A.Z. hat der Vorstandsvorsitzende der Deutschen Bank, John Cryan, die IT-Systeme seiner eigenen Bank als »lausig« bezeichnet.[149] Von dort allerdings sind bislang keine spektakulären digitalen Einbrüche bekanntgeworden. Anders sieht es etwa bei der NASDAQ – der größten US-Technologiebörse – aus, die am 22. August 2013 für einen halben Tag geschlossen werden musste. Niemand hat den Kunden wie Anlegern bis heute glaubhaft erklärt, was dort eigentlich passierte. Gold-Experte und Bestseller-Autor James Rickards, den Sie bereits im Gold-Kapitel näher kennengelernt haben, vermutet dahinter keine normale Computerpanne, sondern einen Cyber-Angriff, entweder von kriminellen Hackern oder sogar chinesischen oder russischen Militärs.[150]

Egal ob sie auf eigene Rechnung handeln oder im staatlichen Auftrag – Banden kommen heute nicht mehr mit Pistolen oder Schneidbrenner, sondern mit IT-Programmen und -Gerätschaften, die hochgradig professionell, manchmal aber so simpel wie ein Brecheisen sind. Cyber-Angriffe haben stark zugenommen, weltweit sind die IT-Sicherheitsvorfälle 2015 gegenüber dem Vorjahr um 38 Prozent gestiegen.[151] Kein Wunder, dass die Kommunikationssicherheit bei den Aufsehern ganz oben auf der Agenda steht. Die Chefin der amerikanischen Börsenaufsicht SEC, Mary Jo White, bezeichnete den Mangel an Cyber-Sicherheit als das größ-

te Risiko für die Finanzstabilität. Dabei hat sie nicht nur die Banken im Blick, sondern auch Börsen, Handelsplattformen und Wertpapierabwicklungshäuser. Hier sieht die SEC-Chefin einen hohen Nachholbedarf zur Erhöhung der Systemsicherheit. Die Lage ist so ernst, dass die Deutsche Bundesbank in ihrem Bericht zur Finanzmarktstabilität warnt: »Cyber-Risiken resultieren aus Angriffen auf Daten und IT-Systeme und können deren Vertraulichkeit, Integrität und Verfügbarkeit gefährden. (...) Mittels Cyber-Angriffen können des Weiteren Falschinformationen verbreitet und etwa Aktienkurse manipuliert werden.«

Dabei sind naturgemäß vor allem Attacken auf systemrelevante Akteure bedeutsam. Ausfälle in diesem Bereich können das gesamte System ins Wanken bringen – etwa wenn existenzielle Dienstleistungen oder Transaktionen zwischen Banken nicht mehr angeboten werden können. So ist es möglich, dass Liquiditäts- und Kreditrisiken entstehen und sich im Finanzsystem ausbreiten. Natürlich können Cyber-Angriffe auch die Reputation einschlägiger Organisationen beschädigen und das Vertrauen der Kunden erschüttern. Und dies muss nicht einmal eine Folge eines Betrugs sein. Auslöser dafür können auch Gerüchte sein, die zielgerichtet in sozialen Netzwerken oder den oft obskuren Internet-Finanzportalen gestreut werden. Dort finden sich auch Erpresser »alter Schule« wieder, die die klassische Schutzgelderpressung mit den Möglichkeiten des Internets verknüpfen und vorsätzlich falsch über Finanzprodukte informieren, sollte der Anbieter keinen gut dotierten Beraterauftrag an sie vergeben. Der 2010 verstorbene Heinz Gerlach etwa hat auf diese Weise Emissionshäuser drei Jahrzehnte lang erfolgreich erpresst – obwohl er mehrfach einschlägig verurteilt wurde. Leute mit ähnlichen Praktiken sind immer noch unterwegs. Zwar sind die Effekte hier nicht unbedingt systemrelevant, aber für den jeweiligen Fondsanbieter allemal gravierend. Eine konzertierte Schmierenkampagne – etwa eine Gerüchtekampagne, dass eine bestimmte Bank insolvenzgefährdet sei – kann rasch zu einem Ansturm auf das Geldhaus führen.

Während sich die bösen Phantasien von Erpressern, oft Marktteilnehmern, nicht durch staatliche Auflagen aus der Welt schaffen lassen, sondern nur durch den langwierigen und kostspieligen Rechtsweg (bei Heinz Gerlach half nicht einmal das), gibt es für den technischen Aspekt dieses Themas harte Vorgaben: Inzwischen überprüfen die Bankenaufsicht und die Bundesbank nicht mehr nur die Liquidität und Kompetenz eines Finanzdienstleisters, sondern auch dessen Vorkehrungen gegen Cyber-Risiken. Schließlich ist der Schutz gegen solche Attacken genauso wichtig wie die Hinterlegung von Eigenkapital und Kreditsicherheiten. Bis hin zum Bundesamt für Sicherheit in der Informationstechnik (BSI) reicht die Liste der involvierten Institutionen. International kümmern sich unzählige Gremien um den IT-Schutz – so zum Beispiel die *Bank für Internationalen Zahlungsausgleich* und dort der *Ausschuss für Zahlungsverkehr und Marktinfrastrukturen*, die *Internationale Vereinigung der Wertpapieraufsichtsbehörden* und sogar eine Arbeitsgruppe der G7-Länder. Das ist aber nicht immer mit dem entsprechenden Erfolg verbunden, wie wir gleich sehen werden. Die G7-Kommission hat Grundelemente zur Cyber-Sicherheit für den Finanzsektor entwickelt, die Ende 2016 von den Finanzministern und Notenbank-Gouverneuren der G7-Staaten verabschiedet wurden. Das Thema Cyber-Sicherheit hat schließlich auch die Bankenaufseher der EZB auf den Plan gerufen. Sie wollen eine Datenbank über Cyber-Angriffe einrichten.[152] Trotzdem kommen die Einschläge näher, denn allzu verlockend ist es offenkundig für Verbrecher, mit ausgeklügelten Programmen 100 Millionen Dollar auf der anderen Seite des Globus zu erbeuten.

Die Attacke auf Großbanken in den USA 2012

Ein konzertierter Angriff, der die Computernetzwerke überlasten sollte, traf 2012 gleich mehrere Großbanken der USA: Darunter waren Chase, Wells Fargo, die Bank of America und etliche andere. Zur damaligen Zeit war es die teuerste derartige Attacke – allerdings »nur« mit großem wirtschaftlichen Schaden. Weder Geld

noch Kundendaten wurden gestohlen. Die Banken verloren viel Geld, weil die Systeme repariert werden mussten und ihre Kunden keine Bankgeschäfte tätigen konnten – das Ganze glich einem Einbruch, bei dem die Verbrecher zwar das Haus verwüsten, aber nichts mitnehmen. Auch hier erfolgte die Attacke mit vereinter Kraft über gekaperte Server, die einen plötzlichen und vielfachen Datenzugriff auf die Banken ausführten. In der Folge dieses sogenannten *Distributed Denial of Service (DDoS)* mussten die Netzwerke den Dienst einstellen.

Der Cyber-Angriff auf Banken und Geldautomaten in Südkorea 2013

2013 legte ein Schadprogramm namens »DarkSeoul« Banken und Geldautomaten in Südkorea lahm. Auch TV-Stationen waren betroffen, und so sorgte die Software nicht nur für Stillstand im öffentlichen Leben, sondern auch für Unruhe und Chaos. Diese Attacke wurde, anders als die anderen Beispiele, außerordentlich simpel ausgeführt: Die Antivirus-Programme der Zielrechner wurden ausgeschaltet, dann wurden deren Daten gelöscht und die Geräte schlichtweg heruntergefahren. Äußerst ungewöhnlich war jedoch, dass gleichzeitig völlig unterschiedliche Betriebssysteme beeinträchtigt waren, nämlich Windows und Linux.

Der größte Bankraub weltweit: eine Milliarde Dollar (2013 – 2015)

Viel weniger bekannt ist paradoxerweise der bislang größte Bankraub im Netz (und wohl auch der größte überhaupt), bei dem offenbar eine Milliarde Dollar vor allem in Russland und den USA illegal den Besitzer wechselte. Bei der Aufklärung tat sich das auf Sicherheitssoftware spezialisierte russische Unternehmen Kaspersky hervor, das mit den Strafverfolgungsbehörden zusammenarbeitete. Dem Raub war eine zwei Jahre andauernde, weltweit organisierte und koordinierte Attacke auf 100 Banken in 30 Ländern vorausge-

gangen. Der Gangster-Ring, der nicht zum ersten Mal zugeschlagen hatte, erhielt von den Experten den Namen *Carbanak*.

Die multinationale Gruppe setzte ein Schadprogramm ein, das Monate vor dem Diebstahl auf die Rechner von Systemadministratoren und Bankmitarbeitern geschleust wurde. Nachdem die Software installiert war, konnten die Rechner aus der Ferne so manipuliert werden, dass sich die Gangster, besser gesagt deren Computer, als Bankangestellte ausgeben und Transaktionen vornehmen konnten. Die »Inkubationszeit« wurde vor allem dazu genutzt, zu lernen, wie die Systeme, der Zielrechner und deren Anwender arbeiten. Mit diesem Wissen konnten die Cyber-Gangster daraufhin den Raub ausführen. In einem Fall erbeuteten sie sogar über zehn Millionen US-Dollar.

Das Vorgehen war sehr geschickt, anpassungsfähig, leider erfolgreich und in jedem Fall hollywoodreif. Wie immer fragt man sich unwillkürlich, wie viel Sinnvolles man mit solch einer hohen kriminellen Energie erreichen könnte, die hier mit großer Professionalität und Kreativität gepaart war. In einigen Fällen hatten sich die Hacker sogar Zugang zum System der Geldautomaten verschafft. Sie fuhren daraufhin natürlich nicht persönlich vor, um das Geld aus dem Schlitz zu ziehen. Angesichts der anvisierten Summen hätte das Abheben auch lange gedauert. Vielmehr wurden die Beträge ebenfalls auf ihre Zielkonten gelenkt. Hierfür verwendeten sie nicht einmal Schadsoftware, sondern Standardwerkzeuge, mit denen sich Geldautomaten kontrollieren und testen lassen. Hinzu kam, dass sie bewährte Fernwartungs-Programme nutzten, die sogar auf anerkannten Listen standen und daher nicht auffielen. Die Angreifer verschafften sich so einen derartigen Zugang zum internen Banknetzwerk, dass sie sogar über die Videoüberwachung die Systemadministratoren beobachten und sehen konnten, was diese taten und was sich auf deren Monitoren abspielte. All dies zeichneten sie über Monate hinweg auf.[153]

Beängstigend, dass alles erst aufflog, als sie mit der Beute verschwunden waren. Kriminelle im vordigitalen Zeitalter mussten dafür zumindest Wochenenden und Feiertage nutzen, während es

heute offenbar möglich ist, monatelang quasi unter den Augen der Opfer den eigenen Verbrechen nachzugehen.

Der Angriff auf die russische Zentralbank Ende 2016

Unbekannte Hacker erbeuteten Anfang Dezember 2016 von Russlands Zentralbank zwei Milliarden Rubel (29,2 Millionen Euro). Mittels gefälschter Zugangscodes räumten sie die Konten ab. Durch den russischen Inlandsgeheimdienst FSB konnten jedoch größere Cyber-Anschläge auf das Bankensystem Russlands verhindert werden, die in einer zweiten Welle erfolgen sollten.[154]

Immer wieder, auch hier, stellt sich die Frage: Wer steckt dahinter? Natürlich sind die einheimischen Behörden schnell mit Verdächtigungen zur Stelle, die vor allem in Richtung der traditionellen politischen Feinde zielen. Doch naturgemäß lässt sich dies selten nachweisen, da für die Gauner das Verwischen von Spuren ein wichtiger Teil ihrer Arbeit ist.

Der SWIFT-Angriff in Bangladesch und Vietnam im Jahr 2016

Via SWIFT – dem internationalen Zahlungsverkehrssystem der Banken – wurden Anfang 2016 erfolgreich 81 Millionen US-Dollar von der Zentralbank Bangladeschs abgezogen. Dies lag zwar an mangelnden Sicherheitsvorkehrungen, viel beunruhigender ist allerdings die Tatsache, dass sich all dies eben über SWIFT abspielte, das von Hackern angegriffen worden war. Die Genossenschaft, die durch die Banken weltweit getragen wird, musste schließlich ihre Kunden warnen. SWIFT räumte ein, dass eine Schwachstelle in der Kundensoftware die Ursache war – ein Update wurde nötig.

Ursprünglich wollten die digitalen Bankräuber, die leider ganz real waren, auf elektronischem Wege sogar 951 Millionen Dollar erbeuten und hatten dazu bereits entsprechende Aufträge angewiesen. Ein großer Teil der Überweisungen wurde allerdings blockiert, am Ende fehlten »nur« 81 Millionen US-Dollar. Den Erkenntnissen zufolge hatten die Computer der Zentralbank ernsthafte Sicher-

heitsmängel.[155] Das erscheint noch untertrieben, offenkundig wurden gebrauchte Router für nicht einmal zehn Dollar in der Zentralbank eingesetzt, die über keinerlei Firewall verfügten.[156] Am Ende trat der Zentralbank-Chef nach dieser Blamage zurück.

Auch die vietnamesische Tien Phong Bank erhielt Ende 2016 betrügerische Anfragen zur Überweisung von mehr als einer Million Euro. Es gibt Theorien, wonach die Hacker in Nordkorea zu finden sind, was man auch bei den Angriffen auf Südkorea 2013 vermutet. Bewiesen ist dies allerdings nicht. In Vietnam, genauso wie in Bangladesch, wurde für den Diebstahl ebenfalls SWIFT genutzt. Dem SWIFT-Verbund sind mehr als 10.000 Banken in der ganzen Welt angeschlossen, und er nimmt für internationale Überweisungen eine Schlüsselrolle ein. Die als Kooperative organisierte Institution sitzt in Brüssel und wird von 3.000 Finanzinstituten betrieben. Ihr Auftrag besteht darin, Zahlungsvorgänge weltweit abzuwickeln – und zwar sicher.

Über SWIFT versenden die Institute normalerweise verschlüsselte Nachrichten, die grenzüberschreitende Zahlungen und andere Transaktionen bewerkstelligen. Doch die Cyber-Angriffe mittels dieser SWIFT-Nachrichten beunruhigen nun die Banken. So hat die amerikanische Großbank JP Morgan nach einem Bericht des Wall Street Journal den Zugang zu SWIFT auf bestimmte Berechtigte beschränkt. Auch in anderen Häusern stehen die SWIFT-Systeme derzeit auf dem Prüfstand, dazu dürfte auch die Deutsche Bank als eine der größten Transaktionsbanken in der Welt zählen. Die F.A.Z. schreibt denn auch: »Die wichtigen SWIFT-Kunden, darunter amerikanische und europäische Banken, erwarten nach den jüngsten Fällen verstärkte Sicherheitsvorkehrungen. Offenbar wird befürchtet, dass sich die nächsten Hackerangriffe nicht mehr auf Banken in Entwicklungsländern beschränken werden. Zweifel an der Sicherheit wären für SWIFT ein Desaster.«[157] Denn die Attacken lassen auf sehr gute Kenntnisse der bankinternen Systeme schließen. Dabei soll Spionage-Software (Malware) in den PDF-Reader der Banken eingeschleust worden sein. Nach einem Bericht verfügten die Hacker auch über geheime SWIFT-Kürzel für

mindestens sieben andere Banken. Dabei erinnert die Reaktion von SWIFT ein wenig an die Probleme, die Bitcoin hatte: Nach Angaben von SWIFT ist das eigene System nicht betroffen, die Banken sollten jedoch ihre bankeninternen Sicherheitsvorkehrungen bei den Überweisungssystemen prüfen.[158]

Zwischenfazit

Der Finanzsektor ist von funktionierender IT abhängig. SWIFT ist dabei ein Symbol für unsere vernetzte Welt – und deren Verwundbarkeit. Zwar gibt es rund 200 Nationalbanken und Zehntausende von Geschäftsbanken. Wenn aber deren wichtigste Vertreter nur über ein einziges Vehikel miteinander verbunden sind, kann es mit nur einem Angriff einen weltweiten, systemrelevanten Dominoeffekt geben. Ich finde diese Tatsache verstörender als die zahlreichen Angriffe auf Newcomer der Bitcoin-Bewegung. Trotzdem stellt niemand dieses System in Frage, zu sehr haben wir uns offenbar daran – und an Betrügereien aller Art – gewöhnt.

Meine Ausführungen zu Cyber-Angriffen haben gezeigt, wie verwundbar die IT-Systeme sind. Generell denkt die Bundesregierung mit ihrem »Konzeption Zivile Verteidigung«, die ich gleich beleuchte, auch an Attacken solcher Art. Sie hat daher allen Betreibern von wichtiger Infrastruktur allgemeine Anforderungen ins Stammbuch geschrieben, die gerade auch für Banken gelten. »Angesichts der Vielzahl potenzieller Ursachen für Ausfälle oder Störungen sollen die Versorgungsdienstleistungen strukturell so angelegt werden, dass das Gesamtsystem trotz Störungen lauffähig und regenerationsfähig ist. Jeder Betreiber soll in seinem Zuständigkeitsbereich freiwillig und eigeninitiativ Verantwortung für ein angemessenes Sicherheitsniveau übernehmen. Der Staat erteilt den Betreibern nach Einschätzung der Erforderlichkeit konkrete Auflagen zur Verbesserung der Resilienz und Sicherheit der Kritischen Infrastrukturen.«[159]

Ob diese Anforderungen auch gegen die Computer-Angriffe extrem kluger, aber fehlgeleiteter IT-Krimineller schützen, sei da-

hingestellt. Gut vorhersehbar war allerdings die Einstellung von James Rickards. Für ihn ist die Bedrohung durch einen Cyber-Finanzkrieg »ein weiterer Grund dafür, physisches Gold zu besitzen: weil es nicht digital ist und weder gehackt noch gelöscht werden kann.«[160]

Was tun in einer Krise?

Im vorigen Abschnitt habe ich dargestellt, welche Katastrophen mitunter heute schon in den IT-Systemen der Banken ablaufen (in Hinblick auf die Summen und den personellen und technischen Aufwand sind das bereits regelrechte Kriege). Im Folgenden möchte ich skizzieren, was uns im realen Leben, in unserem direkten Umfeld, bei einer handfesten Krise passieren kann und wie wir uns am besten darauf einstellen. Dabei bin ich alles andere als ein Apokalyptiker. In meinem Wirken als Unternehmer war und bin ich immer optimistisch. Ich glaube an das Konstruktive im Menschen, weiß aber aus meinen Erfahrungen als Mittelständler auch, dass ich mich auf viele Eventualitäten und Unwägbarkeiten einzustellen habe, um das Schiff in den sicheren Hafen zu bringen. Sollte ich ausgesprochene Schönwetterperioden durchfahren (was bei unternehmerischen Herausforderungen selten der Fall ist), so ist das wunderbar; zieht aber ein Sturm auf, bin ich froh, die richtige Ausrüstung und eine kompetente Mannschaft an Bord zu haben. Im übertragenen Sinne sind dies Versicherungen, und so bitte ich auch meine persönlichen Empfehlungen in diesem und im nächsten Kapitel zu verstehen. Bekanntlich ist ein Versicherungsnehmer froh, wenn es nicht zum Schadensfall kommt – umgekehrt jedoch treibt ein Schaden ihn nicht in den Ruin, wenn er eben die Versicherungsprämien regelmäßig gezahlt hat. Bei unseren kommenden Beispielen und Szenarien zur finanziellen Vorsorge im Hinblick auf eine Krise ist nicht einmal die Versicherungsprämie verloren: Sie haben sie geradezu immer in der Hand. Sie verändert zwar mitunter ihren Wert. Aber sie wird ansonsten nicht alt, verliert

mit der Zeit nicht ihre Gültigkeit. Und um das Bild mit dem Schiff noch einmal zu bemühen: Meine empfohlenen Vorkehrungen gegen Stürme müssen auch nicht aufwändig und kostenpflichtig gewartet werden, wie das bei einem Schiff der Fall ist.

»Konzeption Zivile Verteidigung« (KZV) der Bundesregierung

Bevor wir zu den wichtigen privaten Vorkehrungen kommen, sollten wir uns die offiziellen Aktivitäten und Pläne für den Fall von Krisen und Katastrophen anschauen. Schließlich ist es in allererster Linie die Aufgabe des Staates, die Daseinsvorsorge zu verantworten und zu organisieren, ja, die Schutzpflicht hat sogar Verfassungsrang. Auf dem Wissen, dass der Staat im Krisenfall für uns sorgen muss, sollten wir uns aber keinesfalls ausruhen. Schließlich haben wir in den vergangenen Jahren gesehen, wie die aktuelle Bundesregierung wiederholt Gesetze und laut Überzeugung ehemaliger Verfassungsrichter auch die Verfassung gebrochen hat. Das Label *Made in Germany* und unsere weltberühmte deutsche Gründlichkeit haben Kratzer bekommen.

Die »Konzeption Zivile Verteidigung« (KZV) hat viele Bürger im August 2016 überrascht. Glaubten doch viele Deutsche, sie lebten auf einer Insel der Glückseligen. Insofern ist es von der Bundesregierung einerseits verantwortungsvoll, solch ein Konzept vorzulegen, auf der anderen Seite hat es naturgemäß für Verunsicherung gesorgt – etwas, was der zuständige Bundesinnenminister Thomas de Maizière an anderer Stelle schon fast sprichwörtlich vermeiden wollte. Denn die darin beschriebenen Szenarien und Eventualitäten sind für jemanden erschreckend, der in einer Vollkaskogesellschaft aufgewachsen ist.

Praktisch gesehen beschreibt das Konzept umfassend, wie sich alle wichtigen Träger unserer Infrastruktur und Daseinsvorsorge auf den Ernstfall einzustellen haben, und zwar von Krankenhäusern und Sicherheitsbehörden über Stromversorger und Transportunternehmen bis hin zu Banken. Detailliert wird dargelegt, was

unternommen werden muss, wenn etwas passiert. Darunter finden sich selbstverständliche Dinge, die der gesunde Menschenverstand vorgibt, die nun aber in eine feste Form gegossen wurden. Aber auch die einschlägigen rechtlichen Grundlagen und Verpflichtungen, wie das *Post- und Telekommunikationssicherstellungsgesetz* und das *Ernährungsvorsorgegesetz*, sind von der KZV erfasst. Ich empfehle jedem, sich dieses 70-seitige Dokument einmal vorzunehmen und für sich zu überprüfen, was er davon benötigt. Es zeigt nämlich auch, welche Vorkommnisse die Bundesregierung für möglich hält. Denn bislang ist sie nicht als Panikmacherin bekanntgeworden, sondern trat angesichts der Gefahren (auch den von ihr mitverursachten) eher beschwichtigend auf. Gleichwohl sagt all dies nichts über die Wahrscheinlichkeit aus, mit der uns solche Ereignisse treffen können.

Das aktuelle Papier ersetzt die letzte Neukonzeption der Zivilen Verteidigung aus dem Jahr 1995, die noch von der »sicherheitspolitischen Entspannung nach Beendigung des Kalten Krieges geprägt« war. Daraufhin wurden viele bundeseigene Strukturen und Einrichtungen der Zivilen Verteidigung abgebaut. Anlass für die Wiedervorlage lieferten die Terroranschläge in New York und Washington 2001 und das Sommerhochwasser 2002 – was gleichzeitig auch die Bandbreite der möglichen Schadensereignisse aufzeigt. Während die Anzahl der Naturkatstrophen in Deutschland relativ stabil und überschaubar ist, heißt es weiter nur wolkig: »In mehr als zehn Jahren hat sich das sicherheitspolitische Umfeld weiter verändert.«[161]

Die Konzeption Zivile Verteidigung gibt nur die grobe Richtlinie für detailliertere Fachkonzepte vor. Über allem steht dabei das Ziel, »die Staats- und Regierungsfunktionen aufrechtzuerhalten und die Bevölkerung (...) mit den notwendigen Gütern und Leistungen zu versorgen«. Neben den klassisch-militärischen Bedrohungen folgt die KZV der Bedrohungseinschätzung der Bundesregierung und dem »veränderten Sicherheitsumfeld«, wie es im »Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr« beschrieben ist: »Besonderes Augenmerk mit Blick auf

die Landesverteidigung erhielten dabei hybride Bedrohungen sowohl durch staatliche als auch nichtstaatliche Akteure. Es ist die Aufgabe der Zivilen Verteidigung, sich auf die Abwehr dieser neuen Gefahren auszurichten, ohne dabei ihre Aufgaben bei der klassischen Landes- und Bündnisverteidigung zu vernachlässigen. Die wachsende Verwundbarkeit der modernen Infrastruktur und die Ressourcenabhängigkeit moderner Gesellschaften bieten vielfältige Angriffspunkte.«[162] Ausdrücklich werden neben Attacken mit Waffen und Massenvernichtungswaffen auch die im vorangegangenen Abschnitt dargestellten »Cyber-Angriffe und der Ausfall oder die Störung von Kritischen Infrastrukturen« genannt.

Allerdings kann jedem der die KZV liest, bei den beschriebenen »hybriden Bedrohungen« angst und bange werden – zumindest in den Beamtenköpfen des Bundesinnenministeriums scheint unsere heile Welt bereits Vergangenheit zu sein. Die Rede ist von:

- einer Vielfalt offener und verdeckter Angriffe,
- einer Mischung konventioneller und irregulärer Kräfte/Fähigkeiten,
- einer Mischung militärischer und ziviler Wirkmittel,
- der Fokussierung auf verwundbare Strukturen als Angriffsziele,
- der Unübersichtlichkeit potenzieller Schadensszenarien,
- einer erschwerten Wahrnehmung und Zuordnung,
- kurzen oder gänzlich entfallenden Vorwarnzeiten.[163]

Hinzu kommen mögliche Schadensereignisse einer im wahrsten Sinne ganz anderen Natur, nämlich chemischer (C), biologischer (B), radiologischer (R) und nuklearer (N), im Militärjargon zusammengefasst als CBRN.[164] Im Dezember 2015 haben daher die NATO-Außenminister eine Strategie veröffentlicht, wie sie diese Kriegsgefahren bekämpfen wollen. Daran lehnt sich auch die KZV an. Laut NATO-Strategie müssen vor allem folgende Basisfähigkeiten sichergestellt werden:

- Aufrechterhaltung der Staats- und Regierungsfunktionen,

- Versorgung mit Wasser und Nahrungsmitteln,
- Versorgung mit Energie,
- Versorgung mit Kommunikationsleistungen,
- Versorgung mit Transportleistungen,
- Umgang mit Flüchtlingsströmen bzw. Bevölkerungsbewegungen,
- Bewältigung eines Massenanfalls von Verletzten.[165]

Das Bankenwesen oder die Bargeldversorgung aufrechtzuerhalten, diese Aufgabe wird an dieser Stelle nicht genannt. Beide Aspekte werden jedoch später in dem Papier in geeigneter Weise ausgeführt.

Da es mir ein Anliegen ist, in diesem Buch zu ergründen und zu beschreiben, wie wir im Notfall unser tägliches Leben finanzieren, greife ich mir das Thema »Ernährung« als den wichtigsten Aspekt heraus. Einige Aussagen der Bundesregierung werden wir später noch benötigen, daher zitiere ich sie hier ausführlich. So heißt es in dem Konzept:

»Die Regelversorgung mit Nahrungsmitteln erfolgt über eine Vielzahl von Lebensmittelproduzenten und Lebensmittelhändlern ohne besondere Mindestvorgaben. Die Versorgung erfolgt so lange wie möglich durch die privatwirtschaftlich organisierte Lebensmittelwirtschaft über den freien Markt.

Ist nach Feststellung der Bundesregierung eine Grundversorgung der Bevölkerung über den freien Markt nicht mehr gewährleistet, erfolgt eine Versorgung der Bevölkerung mit lebensnotwendigen Lebensmitteln im Wege einer geordneten Produktion und Verteilung der Lebensmittel durch hoheitliche Bewirtschaftung der Lebensmittelerzeugung und Lebensmittelverteilung. Die Bundesregierung kann über den Erlass von Rechtsverordnungen entlang der Lebensmittelwarenkette Verfügungsbeschränkungen und Abgabepflichten hinsichtlich des Anbaus, der Verarbeitung, Verteilung und des Verkaufs von Lebensmitteln erlassen. Darüber hinaus sollen den zuständigen Vollzugsbehörden einstweilige Eingriffsbefugnisse bis zum Erlass entsprechender Rechtsverordnungen

gewährt werden. Die Rechtsgrundlagen für die staatliche Ernährungsnotfallvorsorge sind entsprechend anzupassen.

Zur Sicherstellung der Grundversorgung mit Lebensmitteln kann der Bund eine eigene Nahrungsmittelreserve vorhalten.

Schließlich soll der Selbstschutz der Bevölkerung durch geeignete staatliche Maßnahmen gestärkt werden. Die Bevölkerung wird angehalten, einen individuellen Vorrat an Lebensmitteln für einen Zeitraum von zehn Tagen vorzuhalten, um durch entsprechende Eigenvorsorge die staatlichen Maßnahmen zu unterstützen.«[166]

Leider relativiert eine bedeutende Bundestags-Studie, die ich später vertiefen werde, den Realitätsgehalt dieser Verordnungen deutlich. So heißt es dort: »Der Lebensmittelhandel erweist sich angesichts der erhöhten Nachfrage als das schwächste Glied der Lebensmittelversorgung. Schon nach wenigen Tagen ist mit ernsthaften Engpässen bei der Lebensmittelversorgung zu rechnen. (...) Trotz größter Anstrengungen kann aber mit hoher Wahrscheinlichkeit die flächendeckende und bedarfsgerechte Verteilung der Lebensmittellieferungen nur ungenügend gewährleistet werden.«[167] Eine private Vorsorge – nicht nur mit Lebens-, sondern auch mit Zahlungsmitteln – scheint also dringend nötig zu sein.

Basis des Zivilschutzes ist »die Fähigkeit der Bevölkerung, sich selbst zu schützen und (auch gegenseitig) zu helfen, bis qualifizierte, in der Regel staatlich organisierte Hilfe eintrifft.«[168] Lebenswichtige Grundbedürfnisse sind dabei Trinkwasser, die bereits erwähnte Ernährung und medizinische Versorgung. Erst danach kommen verständlicherweise die Aspekte einer »minimalen Daseinsvorsorge« und auch das Kernthema dieses Buchs:

- Post- und Telekommunikation
- Datenspeicherung und -verarbeitung
- Bargeldversorgung
- Abfallentsorgung
- Abwasserbeseitigung

Bargeldversorgung

Ich weiß nicht, wie die Reihenfolge der »minimalen Daseinsvorsorge« in der Konzeption zustande gekommen ist, immerhin ist sie nicht alphabetisch. Bemerkenswert ist jedoch, dass die Bargeldversorgung zumindest noch vor der Abfallentsorgung und Abwasserbeseitigung auftaucht. Für das Verständnis meiner generellen Ausführungen zum Thema »Geld und Vorsorge«, ja meines grundsätzlichen Konzepts, halte ich es für äußerst wichtig, an dieser Stelle die Regierungsplanung zur Bargeldversorgung vollständig zu zitieren. Zeigt sie doch, was die (theoretischen) Vorgaben für Bundesbank, Kreditinstitute und deren Dienstleister beinhalten – und was eben nicht, sprich: worum man sich selbst kümmern muss:

»Die einzelnen Kreditinstitute haben nach dem Gesetz über das Kreditwesen (KWG) Bankgeschäfte oder Finanzdienstleistungen ordnungsgemäß durchzuführen. Das schließt die Auszahlung von Einlagen ein. Hierfür sind Vorsorgemaßnahmen zu treffen. Derzeit legt jedes Institut für sich fest, welche Risiken in welchem Umfang es als kritisch einschätzt. Sofern ein Kreditinstitut Probleme bei der Bargeldversorgung seiner Kunden als einen für das Institut kritischen Bereich einstuft, muss es entsprechende Notfall- und Krisenpläne (...) vorhalten. Dies gilt dann (...) auch für ausgelagerte Geschäftsfelder, wie zum Beispiel für die Befüllung von Geldautomaten durch Wertdienstleister. Es besteht keine Verpflichtung, für einen betriebsübergreifenden Krisenfall eine Notfallplanung bereitzuhalten, um zur Aufrechterhaltung oder Wiederherstellung des gesamten Bargeldverkehrs beizutragen.

Die Bundesbank sorgt nach § 3 des Gesetzes über die Deutsche Bundesbank (BBankG) für die bankmäßige Abwicklung des Zahlungsverkehrs in Deutschland. Ihr obliegt die Bereitstellung der benötigten bzw. Entgegennahme der abgelieferten Gelder an den Schaltern ihrer 35 regionalen Filialen. Hierzu hält die Bundesbank für ihre Kontoinhaber (Kreditinstitute, Behörden, Zahlungsdienstleister, Personal) Bargeldreserven in allen Stückelungen vor. Darüber hinaus bestehen auf Eurosystem-Ebene strategische Bargeldreserven.

Im Bereich der Bargeldversorgung hat die Bundesbank für ihr Haus sehr umfangreiche Risikovorsorgemaßnahmen, Krisenmanagementpläne und Business-Continuity-Planungen erstellt. Diese Planungen zielen vor allem auf Ad-hoc-Maßnahmen bei kürzeren Krisen (ein bis maximal fünf Tage) ab und verschaffen dadurch Vorlaufzeit für das Ergreifen von Maßnahmen bei längeren Krisen.

Eine unmittelbare flächendeckende Versorgung der Bevölkerung mit Bargeld durch die Bundesbank selbst kann nicht geleistet werden (z. B. wären die derzeit 35 Filialen der Bundesbank – im Vergleich zu aktuell rund 50.000 Geldausgabeautomaten zuzüglich den über 30.000 Bankfilialen – hierfür gänzlich unzureichend, eine Verrechnungs-/Belastungsmöglichkeit im Gegenzug zum einzelnen Bürger besteht nicht). Daher ist eine funktionierende Logistikinfrastruktur (die nicht im Einflussbereich der Bundesbank liegt und die Kreditinstitute sowie die Wertdienstleister einschließt) für eine geordnete Bargeldversorgung der Bevölkerung unbedingt erforderlich.

Die Verteilung des Bargelds an die Bevölkerung erfolgt über die Kreditinstitute, die für den Transport des Bargelds regelmäßig auf Wertdienstleister zurückgreifen. Durch die verstärkte Automation (z. B. automatische Kassentresore in Bankfilialen oder Geldautomaten) können die Auszahlmöglichkeiten im Krisenfall beeinträchtigt sein. Die Sicherstellung der IT-Verfügbarkeit und der Energieversorgung der Kreditinstitute und Wertdienstleister sind daher unverzichtbar. (...)

Vor diesem Hintergrund bedarf es einer Einbindung aller privatwirtschaftlichen Akteure im Bargeldkreislauf (Kreditwirtschaft und Wertdienstleister) in die allgemeine Krisenvorsorge sowie ihrer Verpflichtung zur Mitwirkung in einem die gesamte Bargeldbereitstellung und -entgegennahme (Bargeldverkehr) umfassenden Krisenkonzept.«[169]

Bewertung

Die Überlegungen zur Bargeldversorgung (aber auch die Konzeption insgesamt) empfinde ich aus Sicht eines Staatsbürgers und Unternehmers zunächst als angemessen. Es zeigt, was alles getan werden muss – es zeigt aber auch, wo die Grenzen liegen. Nicht auf alle Eventualitäten und Monstrositäten islamischer Terroristen kann man sich personell und logistisch einstellen – und schon gar nicht gedanklich. Jeder Schadensfall ist einmalig, und wenn es zu einem großen Systemausfall im ganz generellen Sinne kommt (hinter der dann Menschen stehen, es wird sicherlich keine Naturkatastrophe sein), kann niemand heute die Eigendynamik überblicken. Dies kann erst recht nicht eine Privatperson ersehen, aber sie kann das Menschenmögliche tun, und zwar am besten gleich heute, um die Widrigkeiten zumindest abzufedern und ihr Auskommen zu gewährleisten. Was dies im Einzelnen sein kann, werde ich im nächsten Abschnitt und im 6. Kapitel zeigen.

Gleichzeitig ist es beunruhigend, dass die Bundestags-Studie zu den Folgen eines Blackouts auf unsere wichtigen Lebensbereiche ein negatives Grundsatzurteil fällt: »Das behördliche Katastrophenmanagement leidet erheblich unter dem Fehlen eines einheitlichen Lagebilds, sodass auch eine länderübergreifende Planung und Koordinierung von Maßnahmen drastisch erschwert sind.«[170]

Interessant ist übrigens, dass die Bundesregierung die Bevölkerung anhält, Lebensmittelvorräte für zehn Tage anzulegen. Solch ein Hinweis fehlt in der Rubrik »Bargeldversorgung« gänzlich, dabei wäre dies viel einfacher zu bewerkstelligen und benötigt auch weitaus weniger Stauraum als ein 10-Tages-Vorrat an Konserven, Nudeln und Wasser, den ich natürlich für sinnvoll halte.

Wie Sie gelesen haben, macht sich übrigens die Bundesregierung auch über die »Entgegennahme« von Bargeld Gedanken. Zumindest an dieser Stelle halte ich die »Konzeption Zivile Verteidigung« für ziemlich unrealistisch.

Ein Blackout – Ergebnisse einer Studie des Berlin Institute of Finance, Innovation and Digitalization (BIFID)

Im Ernstfall, wenn also die Infrastruktur der Banken mehrere Tage lang ausfällt, ist eine adäquate Versorgung der Bevölkerung mit Bargeld nicht mehr möglich. Das ist das Kernergebnis einer wissenschaftlichen Studie »Alternative Zahlungsmittel im Falle eines IT-Blackouts« des *Berlin Institute of Finance, Innovation and Digitalization*, das sich auf die Untersuchung der Digitalisierung von Wirtschaftsprozessen spezialisiert hat.[171] Der Vertrauensverlust in die Währung, die wir in anderen Kapiteln bislang eher allgemein erwähnt haben, verursacht zudem – unter bestimmten Vorzeichen – eine haltlose Inflation, heißt es in der Untersuchung zu »Alternativen Zahlungsmitteln im Falle eines IT-Blackouts«.

Nicht zu unterschätzen, obgleich nicht Bestandteil der Studie, ist dabei die bereits mehrfach beschriebene Eigendynamik und die allzu menschlichen Reaktionen auf Krisenszenarien: Es gibt einen Run auf Supermärkte, die Menschen hamstern, Nachschub wird kaum noch geliefert – da schließlich die Zahlungssysteme zusammengebrochen sind. Die Waren werden knapp, und in der Folge steigen die Preise.

Wir erleben damit eine klassische Inflation, verursacht durch eine hohe Nachfrage, knappes Angebot und einen Vertrauensverlust in die Währung. Ein Fazit, das die Autoren daraus ziehen, lautet daher: »Edelmetalle schützen vor dem Wertverlust im Ernstfall.«

All dies sind natürlich Szenarien, und wie bei einer Hausratsversicherung, die im Falle eines Einbruchs hilft, wünschen wir uns, dass es nie dazu kommt. Doch es ist leicht, fast so wie ein Versicherungsabschluss per Mouseklick, sich dagegen zu wappnen – mit einer passenden Mischung verschiedener Währungen und eben Edelmetall. Hoffen wir, dass wir dies nie brauchen – aber ruhiger schlafen lässt es sich damit schon.

Die Wissenschaftler des Instituts, das zur Berliner *Hochschule für Wirtschaft und Recht (HWR)* gehört, haben Tausende Szenari-

en dahingehend durchgespielt, was passieren kann, wenn das gesamte Bankensystem zum Erliegen kommt. (Gut möglich ist, dass dies durch einen großflächigen Stromausfall verursacht wird – ein »Schadensereignis«, das wiederum eine eigenständige und äußerst umfassende Studie des Deutschen Bundestags ergründet hat, die ich im nächsten Abschnitt vorstelle.) Nicht alle Szenarien führen zwingend zu großer Not, vieles lässt sich schnell reparieren. Doch entscheidend ist die Eigendynamik – und die möglicherweise fatale Mischung verschiedener Faktoren. Denn die Computer und Stromnetze fallen ja in der Regel nicht einfach so aus, sondern weil sie eben jemand angegriffen hat – mit einem bestimmten Zweck oder einer Agenda. Gibt es dann noch Anschläge, wie wir es bereits erlebt haben, ist die Panik nicht mehr weit.

In unserer Zivilisation haben wir uns daran gewöhnt, über alle grundsätzlichen Annehmlichkeiten ständig zu verfügen. Das ist für uns selbstverständlich, also denken wir gar nicht mehr daran, dass dahinter komplexe Systeme und logistische Meisterleistungen stehen. All dies sind Errungenschaften, die wir uns erarbeitet haben und auf die wir stolz sein können. Wir nutzen sie und führen ein modernes Leben, denken aber nicht daran, was passiert, wenn Teile dieser vermeintlichen Selbstverständlichkeiten ausfallen – und es dann zu einem Dominoeffekt kommt.

Unser Bargeldvorrat

Ganze 103 Euro Bargeld trägt statistisch gesehen jeder Bundesbürger bei sich oder hat es zuhause.[172] Ziemlich wenig angesichts der einen Billion Euro, die an Bargeld zirkuliert. Der Großteil jedoch lagert in den Tresoren von Banken und vor allem von Handelsunternehmen – oder eben außerhalb des Euro-Raums. Wenn für einige Stunden die Geldautomaten und das Kartenlesegerät an der Supermarktkasse streiken, ist dies kein Beinbruch (siehe nächster Abschnitt). Was aber, wenn es länger dauert – gepaart mit anderen Ereignissen? Darüber haben sich die Wissenschaftler vom *BIFID* Gedanken gemacht und hochkomplexe Simulationen angestellt, je-

weils für drei, fünf und zehn Chaostage. Ausgangspunkt war die Frage, wie viel Bargeld und in welcher Form notwendig ist, um in einem Zeitraum von bis zu zehn Tagen eine »Datenkrisensituation« zu überstehen, die eine Bargeldbeschaffung einschränkt. Um es vorwegzunehmen: 103 Euro reichen dazu nicht aus – und zwar weder betragsmäßig noch in der Währung Euro.

Hinzu kommt die schlichte statistische Tatsache, dass es sich hierbei um einen Durchschnittswert handelt, dass es also auch viele Leute gibt, die gar nichts im Portemonnaie haben – nicht weil sie etwa arm sind, sondern weil es schon ein paar Tage her ist, dass sie zum letzten Mal am Bankautomaten waren. Die Personen, die 200 oder 300 Euro in der Tasche haben, und zwar hier einmal wortwörtlich, werden ihnen wiederum nicht weiterhelfen können.

Was also ist zu tun? Und was passiert überhaupt mit den Preisen und unserer Lebensmittelversorgung bei einem Blackout?

Dass unser Finanzdienstleistungssektor reibungslos funktioniert, ist eine der zentralen Aufgaben unseres Alltags. In Kapitel 2 habe ich bereits dargestellt, wie feinziseliert und komplex das Geflecht der Kreditinstitute und Dienstleister ist. Dazu gehört das Bankdienstleistungssystem, das den Zahlungsverkehr zwischen Arbeitgebern, Erwerbstätigen, Banken und Kreditnehmern umfasst. Zu den Teilnehmern am Zahlungs- und Datenverkehrssystem gehören Zahlungsleistende, Zahlungsempfänger, Banken, Clearing-Organisationen und Zentralbanken. Obwohl die Anzahl der Banken im System riesig ist, sich Risiken also vermeintlich verteilen, ist die Risikominimierung faktisch eingeschränkt, wie wir es schon bei SWIFT gesehen haben. Denn Banken greifen heute auf Clearing-Zentren und zentralisierte Speicherfarmen zu. Diese sind zwar hochgradig abgesichert– bis eben ein findiger Hacker privat oder im Auftrag einer feindlichen Regierung das Gegenteil beweist. Die Gefahr liegt jedoch auch in der Systemüberlastung durch unfassbar hohe Datenmengen (*Distributed Denial of Service, DDoS*) oder in einem Systemausfall – der intern auftreten kann oder eben von außen hervorgerufen wird.[173] Die

Bedrohung in einer Krise liegt aber nicht unbedingt in einem völligen Zusammenbruch aller Systeme, sagen die BIFID-Wissenschaftler. Vielmehr ist unter diesem Risiko auch der unerwartete Ausfall einzelner, jedoch wichtiger Bestandteile des Bankdienstleistungs- und Datenverkehrssystems zu verstehen.[174]

Bricht all dies zusammen, ist das schlimm. Es liegt auf der Hand, dass dann niemand mehr Überweisungen vornehmen kann und ein Geschäft keine Kreditkarte mehr akzeptiert, weil das Lesegerät keinen Zugang mehr zum Zentralrechner hat. Doch die Menschen kommen auch nicht mehr an Bargeld ran: Die meisten Automaten – und zwar jene, die nicht an eine Filiale und damit an ein Notstromsystem angeschlossen sind – streiken sofort. Natürlich könnte man in diesem Fall auf den bereits erwähnten Schalterbeamten zurückgreifen. Doch selbst wenn alle verfügbaren Kräfte aus den Call-Centern in die Filialen beordert würden, können wir uns lebhaft vorstellen, wie lang die Schlangen wären, wie umständlich und langwierig die Identifikation der Kunden und das Ausfüllen von Formularen wäre. (Genaueres hat die »Bundestags-Studie« durchgespielt, die wir ausführlich im nächsten Abschnitt zitieren.)

Die Versorgung mit Bargeld kommt also zum Erliegen, zumal wir dabei noch nicht über die Tatsache gesprochen haben, dass auch den Banken irgendwann das Geld ausgeht und sie Nachschub benötigen. Zudem werden die Leute so viel Geld wie möglich abheben wollen. Zwar wird hier mutmaßlich schnell ein Limit eingeführt. Aber das lässt sich umgehen, indem sich eben alle Familienmitglieder hintereinander anstellen. Ich muss nicht weiter dieses Bild skizzieren, Sie können sich das Chaos ausmalen, dem wir ausgesetzt sind, nur um wieder flüssig zu sein – etwas, was in den Tagen davor einfach so nebenbei ging und kein großartiges Nachdenken erfordert hat, weil es ein inzwischen automatisierter Vorgang ist.

»Die Funktionsstrukturen des Finanzdienstleistungssektors – verbunden mit der Nutzung moderner internetbasierter Technolo-

gien – lassen die Abhängigkeit von diesen Systemen, aber vor allem deren Risikoanfälligkeit erahnen«, schreiben die Wissenschaftler.[175]

Die große Politik hat sich nicht nur in Bezug auf die zivile Vorsorge dieses Themas angenommen, sondern auch den Stromausfall – der ja einen realistischen Grund für einen Systemausfall und damit quasi ein Angriffsziel darstellen kann – wissenschaftlich flankiert: Unter dem schlichten Titel »Was bei einem Blackout geschieht« hat das *Büro für Technikfolgen-Abschätzung* beim Deutschen Bundestag 2011 die »Folgen eines langandauernden und großräumigen Stromausfalls« untersucht, und zwar für wesentliche Teile unserer Infrastruktur. Eine ihrer Kernaussagen lautet: »Der Finanzdienstleistungssektor ist in hohem Maße von einer kontinuierlichen und stabilen Stromversorgung abhängig. Der Grund sind die für Kommunikation, Datenhaltung, Verfolgung und Regelung der Waren- und Geldströme sowie für den Zahlungs- und Datenverkehr genutzten strombasierten Informations- und Kommunikationsinfrastrukturen. Diese bilden das ›Nervensystem‹ des Sektors. Ein Ausfall dieser Infrastrukturen und die damit einhergehende erschwerte oder verhinderte Erbringung der wesentlichen Finanzdienstleistungen hätten gravierende Auswirkungen auf Wirtschaft und Gesellschaft«.[176] Fallen diese Systeme aus oder funktionieren sie nur noch eingeschränkt, müssen wir also von einer Datenkrise sprechen.[177]

An dieser Stelle kommt das »Konzept Zivile Verteidigung« der Bundesregierung ins Spiel. Wir erinnern uns, dass die einzelnen Kreditinstitute »nach dem Gesetz über das Kreditwesen (KWG) Bankgeschäfte oder Finanzdienstleistungen ordnungsgemäß durchzuführen haben (...) Das schließt die Auszahlung von Einlagen ein. Hierfür sind Vorsorgemaßnahmen zu treffen.«[178] Nach diesem Konzept legen somit Kreditinstitute die Bargeldversorgung selbständig fest. Das aber müsste im Hinblick auf die Finanzkrise 2008, die chronische Euro-Krise und die damit verbundene Bargeldversorgung der griechischen Bevölkerung im Jahr 2012 sicherlich kritisch nachgefragt und geprüft werden, wie die BIFID-Autoren bemerken.[179]

Zwar beträgt das private Netto-Geldvermögen je Einwohner in Deutschland 47.681 EUR.[180] Dies zeugt zunächst von einer vernünftigen Bonität (im Vergleich zu anderen Ländern). Doch das hilft einem Bürger nichts, denn er kann während einer Krise nicht darauf zugreifen. Damit wäre der Lehrsatz aus den finanzwirtschaftlichen Büchern »Liquidität folgt Bonität« außer Kraft gesetzt, stellen die BIFID-Experten lakonisch fest. Im Umkehrschluss heißt das: Was zählt, ist Cash. Bundesbank und Geschäftsbanken würden eine ordnungsgemäße Versorgung im Krisenfall kaum bewerkstelligen können, Bundesbankgesetz und »Konzept Zivile Verteidigung« hin oder her. Das schreiben auch die Autoren des Büros für Technikfolgen-Abschätzung. Doch was passiert dann? Dazu gleich mehr im nächsten Abschnitt.

Alternative Zahlungsmittel

Laut der Definition der Deutschen Bundesbank wird als »gesetzliches Zahlungsmittel« das Zahlungsmittel bezeichnet, »das niemand zur Erfüllung einer Geldforderung ablehnen kann, ohne rechtliche Nachteile zu erleiden. Im Euro-Raum ist Euro-Bargeld das gesetzliche Zahlungsmittel.« Als alternatives Zahlungsmittel kann also Bargeld oder Bargeldersatz verstanden werden, das bzw. den niemand zur Erfüllung einer Geldforderung ablehnen würde.[181] Doch welche sind das? Die BIFID-Studie hat dies ebenfalls untersucht und praktische Lösungen vorgeschlagen.

Ob ein alternatives Zahlungsmittel zum Einsatz kommt, hängt von dem Vertrauen in ein Zahlungsmittel und von dessen Kaufkraft ab – beides ist, wie Sie sich erinnern, der Kern einer Währung und deren Akzeptanz. Denn sollte es zu einer Vertrauenskrise in das gesetzliche Zahlungsmittel kommen, lässt sich aus der Vergangenheit in verschiedenen Inflations-Konstellationen herleiten, welche Reaktionen dies voraussichtlich in der Bevölkerung hervorruft. Vor allem in Deutschland wären die Inflationsfolgen dramatisch, denn das Trauma der mehrfachen Geldvernichtung während der

Inflationszeit hat sich bis heute tief in die deutsche Seele eingegraben. Und so zeichnen die Wissenschaftler mehrere Szenarien:

1. Nutzung einer anderen, also alternativen Währung, die noch mit Vertrauen ausgestattet ist, etwa US-Dollar, Schweizer Franken oder Britisches Pfund
2. Nutzung von Wertgegenständen, wie Schmuck, Briefmarken oder Bilder
3. Nutzung von Edelmetallen, also Gold oder Silber bzw. von Diamanten
4. Nutzung von Gütern, das waren in der Nachkriegszeit oft Zigaretten, die auf dem Schwarzmarkt gegen »sinnvolle« Verbrauchswaren eingetauscht wurden.[182]

Im Kaptal 2 habe ich nicht nur die bunte Geschichte von Bargeld beschrieben, sondern auch einige recht ungewöhnliche Zahlungsmittel. Als nachhaltig haben sich davon kaum welche erwiesen: Schmuck, Briefmarken oder Bilder – das ist nicht nur exotisch, sondern auch unpraktisch. Ersatzgüter wie Zigaretten sind zwar prinzipiell denkbar, und wurden mit der Sorte *Kent* auch lange in Rumänien eingesetzt. Doch stellt sich hier ebenfalls rasch die Frage nach einem Standard, also einer Art Konvertierbarkeit – ein Punkt, den wir noch mehrfach antreffen werden. Die Wissenschaftler haben sich also auf die Zahlungsmittelszenarien 1. (Alternativwährungen) und 3. (Edelmetalle) konzentriert; diese sind aus ihrer Sicht am wahrscheinlichsten.

Doch schon bei einer Alternativwährung fangen die Probleme an. Welche nehmen wir denn? Schließlich sprechen wir von Krisenzeiten und nicht von einer Schönwetterperiode. So galt das Britische Pfund über lange Zeiträume als eine der Leitwährungen der Welt. Doch die Zeiten sind lange vorbei, in denen es hieß, »wenn das Pfund hustet, bekommt Europa die Schwindsucht.« Nicht nur das Empire, in dem die Sonne nie unterging, ist zusammengeschmolzen, sondern auch der Wert des Britischen Pfunds. Es ist zwar immer noch eine anerkannte Wäh-

rung, aber Ereignisse wie die Brexit-Entscheidung im Sommer 2016 haben uns gezeigt, wie schnell das Pfund in die Bredouille geraten kann. Auf der anderen Seite ist das Pfund naturgemäß eine Alternative zum Euro. Warum es also nicht in einer bestimmten Stückelung zu den heimischen Reserven hinzufügen?

Die Stärke und Solidität des Schweizer Franken ist dagegen sprichwörtlich. Zumindest mit Blick auf die Vergangenheit, darf man behaupten, dass er mehr als ein harter Notgroschen ist. Dagegen schwankt der Dollar stets, ist aber zugleich die Leitwährung Nummer 1 mit großem Abstand zum Euro. Welche alternative Währung bei einem Bargeldengpass jedoch allgemein akzeptiert wird – und darauf kommt es an, es wird sicherlich nicht mehrere gleichberechtigte Möglichkeiten parallel zueinander geben –, vermag auch ich nicht zu prognostizieren. Somit sollte jeder eine Mischung parat haben.

Spätestens an dieser Stelle können wir uns endlich wieder dem Thema Gold widmen: Seine unumstößliche Bedeutung in unserer Kultur und in (früheren) Währungssystemen habe ich mehrfach dargelegt. Es ist der rote Faden des Buchs und somit auch ein logischer Schritt, das Edelmetall in die private Vorsorge mit aufzunehmen.

Historisch hat Gold seine Funktion als Zahlungsmittel oder Verrechnungsgröße nur in den vergangenen 45 Jahren eingebüßt, ansonsten war es vor der Erfindung von Papiergeld, elektronischen Überweisungen oder virtuellen Bitcoins gewissermaßen *das* Zahlungsmittel schlechthin. Der Werterhalt und auch die Fungibilität von Gold sind historisch bewiesen, seine Eigenschaft als Tauschmittel in Zeiten von Unsicherheit ist anerkannt und steht außer Frage.

Das entscheidende Problem jedoch ist die Teilbarkeit und die Bestimmbarkeit in kleinen Mengen. Es ist offenkundig, dass etwa Goldschecks oder bei einer Bank eingezahlte Goldguthaben nicht im Barverkehr akzeptiert werden. Hingegen liegt die kleinste »ver-

nünftig« handelbare Einheit bei einem Gramm, was heute etwa 36 Euro entspricht.

Simulation eines Zahlungsausfalls

Die BIFID-Spezialisten haben eine Situation simuliert, in der ein technisch bedingter Ausfall von Zahlungssystemen entsteht – und es somit zu massiven Problemen bei der Bargeldversorgung kommt. Sie haben dabei, wie das üblich ist, verschiedene Annahmen vorgenommen. Im Mittelpunkt der Untersuchung steht einzig und allein die Nahrungsmittelversorgung. Andere lebenswichtige Ausgaben wurden hier nicht durchgespielt, wobei die Gesundheitsversorgung der Einfachheit halber als gewährleistet angenommen wird.

Die Wissenschaftler unterstellen – so wie die Bundestags-Studie auch, aber anders als das Bundesinnenministerium –, dass die Logistik für die Nahrungsmittelversorgung nicht mehr funktioniert und dass nur die im Handel vorhandenen Lebensmittelvorräte zur Verfügung stehen. Diese Tatsache wird in der Simulation damit abgebildet, dass es je nach den verfügbaren Lebensmittelmengen zu Preissteigerungen kommen kann.

Die entscheidenden Faktoren bei dieser Simulation sind also die dynamischen Preissteigerungen, die Preiselastizität, die vorhandene Nahrungsmittelmenge, die durchschnittlichen täglichen Pro-Kopf-Ausgaben für Nahrungsmittel sowie die Länge des Ausfalls der Bargeldversorgung.[183] Herausgekommen ist ein mehrdimensionales Modell, das darauf abstellt, ob und wie lange die 103 Euro pro Person ausreichen. Insgesamt wurden 9.100 mögliche einzutretende Situationen analysiert, die sich aus der Kombination von abnehmender Gütermenge und zunehmender Preiselastizität abbilden lassen. Die Preiselastizität misst die Änderung des Angebots oder der Nachfrage nach einer Preisänderung. Je höher die Preiselastizität, desto stärker reagiert die Menge auf die Preisänderung.[184]

Das betrachtete Zeitfenster haben die Autoren auf bis zu zehn Tage festgesetzt. Zudem wird der kumulierte Eurobetrag als Zielvariable formuliert, der über das analysierte Zeitfenster benötigt wird. Die verfügbare Nahrungsmittelmenge wird in ihrer Entwicklung von einem Niveau von 100 Prozent auf ein Niveau von ein Prozent betrachtet. 100 Prozent bedeutet also eine lückenlose Versorgung bezogen auf den täglichen Kalorienbedarf mit Lebensmitteln. Die Nahrungsmittelmenge beeinflusst somit über die Elastizität das Preisniveau der Nahrungsmittel. Eine Verknappung des Angebotes an Nahrungsmitteln führt naturgemäß zu einem Anstieg des Preises.

Die durchschnittliche Tagesausgabe pro Person für Nahrungsmittel beträgt statistisch gesehen 6,47 Euro.[185] Bei einem Zwei-Personen-Haushalt belaufen sich also die monatlichen Ausgaben für Nahrungsmittel, Getränke und Tabakwaren auf 388 Euro. Haushalte mit Kindern dürften dabei tendenziell eher höhere Ausgaben haben.

Simulationsergebnisse

Wir haben also ein fünfdimensionales Modell, bestehend aus Preiselastizität (Veränderung von Angebot und Nachfrage vor dem Hintergrund von Preisveränderungen), der Gütermenge, dem Preisniveau, dem bis zu zehn Tage umfassenden Zeitintervall und den im Durchschnitt verfügbaren 103 Euro pro Person. Zur besseren Verständlichkeit, und weil dies auch die alles beherrschende Frage beantwortet, steht im Mittelpunkt, ob und wie lange die 103 Euro ausreichen. Die Antwort ist abhängig von der Preiselastizität und der vorhandenen Gütermenge.

Die Simulationsergebnisse zeigen: Je nach eintretender Situation wird die in bar vorhandene Liquidität nicht ausreichen, damit sich die Bundesbürger mit Nahrungsmitteln über einen bestimmten Zeitraum versorgen. Naturgemäß verändert sich die Situation mit fortschreitender Zeit deutlich. Bei drei Tagen ist die Lage noch sehr entspannt. Die Wissenschaftler kommen nur in zehn

von 9.100 Szenarien auf eine Situation, in der die privaten Bargeldreserven von 103 Euro nicht genügen. Ähnlich undramatisch sieht es bei fünf Tagen aus: Lediglich in einigen extremen Situationen, und zwar in 27 von 9.100 Fällen, ist die vorhandene Liquidität von 103 Euro vorzeitig erschöpft.[186] Bei einem Zahlungsausfall von zehn Tagen finden die BIFID-Experten immerhin schon 133 Szenarien, bei denen das vorgehaltene Bargeld nicht ausreichend ist.

Doch die generellen und zunächst recht entwarnenden Simulationsergebnisse berücksichtigen dabei nicht, dass das Vertrauen in die Währung verloren geht und somit die Preise entsprechend steigen. In einer gesonderten Betrachtung haben die Experten dieses Szenario einbezogen – mit dem naheliegenden Ergebnis, dass die Barreserven seltener ausreichen. Bei 64 Prozent aller Szenarien, also in 5.800 von 9.100 Fällen, reicht dann der durchschnittlich vorhandene Bargeldvorrat nicht mehr aus. Die Folgen sind drastisch: Schrumpft die Nahrungsmittelmenge auf ein Viertel des Ursprünglichen, werden dafür Ausgaben benötigt, die hochgerechnet auf zehn Tage stolze 680 Euro ausmachen. Für das letzte Zehntel einer gegebenen Nahrungsmittelmenge müsste man 1.894 Euro bezogen auf zehn Tage berappen. Angesichts von 103 Euro, die ursprünglich vorhanden sind, ist es offenkundig, dass man damit nicht weit kommt – unter bestimmten Annahmen wohlgemerkt.

Empfehlungen

Eine verbindliche Empfehlung geben die Autoren der Studie zwar nicht ab, sie treffen aber neutrale, und damit folgerichtig schwerwiegende Aussagen. Jeder Leser kann daraus seine eigenen Schlüsse ziehen: »Wenn es zu einer absehbaren, endlichen Datenkrise kommt, die das Vertrauen in die Währung nicht erschüttert, sollten die vorgehaltenen Barreserven ausreichend sein.« Doch weiter heißt es: »Nähme ein Autor aber die Entwicklungen der letzten Jahre mit in die Betrachtung auf und analysiert nicht nur quantitativ, sondern ggf. auch mit Einschätzungen, wäre es u. U. sinnvoll, höhere Bestände an Bargeld vorzuhalten. Käme es dann noch

zu einem Vertrauensverlust in die lokale Währung, könnte es als sinnvoll betrachtet werden, Sorten einer/mehrerer Währung(en) vorzuhalten. Da auch hier Veränderungen in der Einschätzung vorliegen könnten, ist eine Aussage, welche Sorten vorzuhalten sind, schwierig. Um dieses Risiko ggf. zu minimieren, könnte eine Vorsorge darin bestehen, Edelmetalle vorzuhalten.«[187]

Die Autoren legen dabei nahe, eben jenen Betrag von 1.894 Euro verfügbar zu halten, mit dem man im Worst-Case-Szenario zehn Tage lang auch bei massiven Preissteigerungen über die Runden kommt. Vor dem Hintergrund eines durchschnittlichen Vermögens von 47.681 Euro erscheint dies machbar. Die Frage ist nun: In welcher Form sollte man diese 1.894 Euro vorhalten?

Im Verlauf der Finanzkrise 2008 gab die Bundesregierung erstmalig eine Staatsgarantie für alle Spareinlagen privater Anleger ab, die im weiteren Verlauf ihren Eingang in das Einlagesicherungsgesetz gefunden hat. Ziel war es, den Run auf die Banken zu verhindern und eine unkontrollierte Abhebung von Bargeld zu unterbinden.

Heute sehen wir uns schließlich mit genau jenen Herausforderungen konfrontiert, die in diesem Buch und Kapitel eine Rolle spielen: der hohen Abhängigkeit des Finanzsektors von der Funktionsfähigkeit der IT-Systeme.

Die Autoren erweitern daher die bisherigen Empfehlungen, Bargeldreserven zu halten, um weitere Zahlungsmittelformen. Demnach »sollten neben einem Bargeldbestand in Euro, auch eine andere als sicher angesehene und international akzeptierte Währung wie der US-Dollar sowie Edelmetalle wie Gold und/oder Silber (in kleinen Stückelungen) vorrätig gehalten werden.«[188]

Die empfohlene Höhe ist dabei stark abhängig von der Dauer eines IT-Blackouts (dessen Ende niemand voraussehen kann). Sie schlagen jedoch vor, für die in Rede stehenden zehn Tage pro Person einen Gegenwert von 2.000 Euro zu halten – die in etwa zu gleichen Teilen auf die einzelnen Zahlungsmittel verteilt werden. Das heißt, »jede der drei zentral empfohlenen Zahlungsmittel Euro, eine stabile Währung außerhalb der Euro-Zone und Edelmetal-

le sollten zu jeweils einem Drittel vorhanden sein«, so die Finanzexperten. Sie betonen sogleich, dass »ausgehend von der Quelle der Krise, ein Vertrauensverlust in andere Währungen nicht auszuschließen ist. Dies spräche für einen höheren Anteil von Edelmetallen in kleinen ›handelbaren‹ Stückelungen.«[189]

Gold gehört also in den privaten Vorsorgekorb, sagen die Wissenschaftler. (Zwar reden sie allgemein von »Edelmetall«, doch sind damit nur Gold und Silber gemeint, und Silber ist eindeutig zweite Wahl.) Es liegt auf der Hand, dass dazu aber nicht das heimische Zahngold, das Erbstück der Oma oder Goldmünzen geeignet sind. Denn damit kann ich im Ernstfall schlecht Brot kaufen. In welcher Form uns Gold also in solchen Situationen pragmatisch hilft, werde ich in den kommenden beiden Kapiteln aufzeigen.

Vorher jedoch möchte ich die bereits mehrfach erwähnte Bundestags-Studie zum »Blackout« vorstellen. Sie ist erst einige Jahre alt, enthält aber starken Tobak. Denn was zum Zeitpunkt ihrer Entstehung eher wissenschaftliche Theorie war und in den Schubladen verschwunden ist, ist momentan leider aktueller denn je geworden. Sie ergänzt damit die Überlegungen zu einem IT-Blackout hervorragend.

Exkurs: »Bundestags-Studie zum Blackout«

»Was bei einem Blackout geschieht. Folgen eines langandauernden und großflächigen Stromausfalls.« Studie des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), 2011.

Im vorangegangenen Abschnitt habe ich dargelegt, wie weit wir im Fall eines Blackouts mit 103 Euro kommen, um uns Lebensmittel zu kaufen. Hintergrund dieser BIFID-Untersuchung ist der potenzielle Zusammenbruch der Bankensysteme – verursacht durch einen IT-Blackout. Einen generellen und längeren Stromausfall, der sich sofort auf alle Infrastrukturbereiche und damit auch auf Banken und deren IT-Systeme drastisch auswirkt, hat 2011 das *Büro*

für Technikfolgen-Abschätzung beim Deutschen Bundestag umfassend untersucht: »Aufgrund der nahezu vollständigen Durchdringung der Lebens- und Arbeitswelt mit elektrisch betriebenen Geräten würden sich die Folgen eines langandauernden und großflächigen Stromausfalls zu einer Schadenslage von besonderer Qualität summieren. Betroffen wären alle Kritischen Infrastrukturen, und ein Kollaps der gesamten Gesellschaft wäre kaum zu verhindern. Trotz dieses Gefahren- und Katastrophenpotenzials ist ein diesbezügliches gesellschaftliches Risikobewusstsein nur in Ansätzen vorhanden.«[190] Verursacht werden kann solch ein langandauernder und regional übergreifender Stromausfall durch technisches und menschliches Versagen, durch kriminelle oder terroristische Aktionen, durch Epidemien, Pandemien oder durch Extremwetterereignisse. Was dann – und die Autoren bezeichnen dies ausdrücklich als Katastrophe – mit unseren Finanzdienstleistungen und der Bargeldversorgung passiert, ist ein Teil der ganzheitlichen Szenarien des bereits erwähnten Reports »Folgen eines langandauernden und großräumigen Stromausfalls«.

Zwar bezeichnen die Autoren das Finanzdienstleistungssystem in einzelnen Teilsektoren als relativ robust: »Nach Einschätzungen von Experten sind der Daten- und Zahlungsverkehr zwischen den Banken, den Clearing-Organisationen und den Börsen, die Datenhaltung sowie weitere kritische Geschäftsprozesse über eine lange Zeit durch Notstromversorgung gewährleistet bzw. können in ein nichtbetroffenes Gebiet ausgelagert werden.«[191] Dagegen werden die Kommunikationswege zwischen den Banken, Clearing-Organisationen und Handelsplätzen einerseits und den Personen und Unternehmen, die Finanzdienstleistungen nachfragen, andererseits als weniger stark eingeschätzt: »Viele Banken, die nach dem Eintritt des Stromausfalls noch geöffnet bleiben, schließen nach einigen Tagen. Da auch die Geldautomaten ausgefallen sind, droht die Bargeldversorgung der Bevölkerung zu kollabieren. Es ist anzunehmen, dass es hierdurch und durch den Ausfall elektronischer Zahlungsmöglichkeiten in Geschäften und Banken mit der Zeit zu

Unmut und teils zu aggressiven Auseinandersetzungen kommt, da es für die Bevölkerung keine Bezahlmöglichkeiten mehr gibt.«[192]

Die fehlenden elektronischen Bezahlmöglichkeiten und die versiegende Bargeldversorgung werden ausdrücklich als »Achillesferse des Sektors«[193] bezeichnet.

Die sehr anschaulichen Szenarien möchte ich an dieser Stelle ausführlich dokumentieren und für sich sprechen lassen. Die Wissenschaftler haben dabei die Folgen jeweils für mehrere Stunden bis hin zu zwei Wochen durchgespielt und anschaulich dargestellt (Fettungen von mir).

Folgen eines langandauernden und großflächigen Stromausfalls für Finanzdienstleistungen (Seiten 173ff.)

Größere Banken, Versicherungs- und Vorsorgeeinrichtungen und andere bankähnliche Organisationen haben sich auf Stromausfälle vorbereitet. Ihr BCM (Business Continuity Management) für den Fall eines Stromausfalls variiert zwar, zeigt aber auch zahlreiche Gemeinsamkeiten (EBP 2010, S.42). In der Regel definieren die einzelnen Geschäftsbereiche innerhalb eines Unternehmens (z. B. Zahlungsverkehr, Anlageverwaltung), welches die kritischen Geschäftsprozesse sind und legen fest, wie sie diese im Fall eines länger andauernden Stromausfalls fortführen wollen. Kritische Geschäftsprozesse sind insbesondere Tätigkeiten rund um Zahlungs- und Datenverkehr, Datenhaltung und Kontenbewegungen, Handel und Wertpapierabwicklung sowie die Versorgung mit liquiden Mitteln (u. a. Bargeldversorgung) (Bankenverband 2004, S. 20 ff.).

Eine grundlegende technische Option, dies sicherzustellen, ist eine entsprechende Notstromversorgung für die essenziellen Informations- und Kommunikationsinfrastrukturen (Server und Datenleitungen), aber auch für die Arbeitsplätze und wichtige Einrichtungen (z. B. Tresore). Zudem ist vielerorts vorgesehen, im Fall eines großflächigen und/oder langandauernden Ereignisses sowohl die Daten als auch die Belegschaft an einen nichtbetroffenen Standort zu verlagern (z. B. in das Ausland, häufig London). Einige Kreditinstitute unter-

halten zu diesem Zweck Ausweichstandorte mit der entsprechenden Kommunikations- und Informationsinfrastruktur in geografisch z. T. weit entfernten Regionen. Zudem verfügen Banken in der Regel über eine gesicherte Notstromversorgung (dieselbetriebene Netzersatzanlage) für etwa eine Woche, wobei für länger dauernde Stromausfälle entsprechende Lieferverträge mit Zulieferern bestehen, die eine Versorgung garantieren sollen. Innerhalb dieses Zeitraums könnten die kritischen Geschäftsprozesse in nichtbetroffene Regionen ausgelagert werden (EBP 2010, S. 12 ff.).

Die jederzeitige Verfügbarkeit von Bargeld ist eine der wichtigsten Finanzdienstleistungen. Eine Nichtverfügbarkeit in einer Krisensituation wird bei der betroffenen Bevölkerung die ohnehin schon vorhandene Unsicherheit weiter erhöhen. Die Nachfrage nach Bargeld dürfte in einer Krisensituation schnell zunehmen, durchschnittlich soll ein Bürger in Deutschland 118 Euro mit sich tragen (Deutsche Bundesbank 2009b, S. 40). Es ist damit zu rechnen, dass bei einem länger andauernden Stromausfall die Verteilung des Bargelds durch Banken und private Wertdienstleister nicht über die ganze Zeit gewährleistet ist. Die Bundesbank gibt aber an, dass zur »Bewältigung eines Not- oder Katastrophenfalls ... spezielle Vorkehrungen im Rahmen einer Krisenmanagementorganisation« getroffen worden sind (BBK 2008a, S. 120).

Null bis zwei Stunden

Der plötzliche Stromausfall führt bei Banken dazu, dass sofort damit begonnen wird, die für das BCM vorgesehenen Maßnahmen umzusetzen. Größere Banken haben in der Regel Vorkehrungen dafür getroffen, dass die zentralen Finanzdienstleistungen (kritische Geschäftsprozesse) durch eine entsprechende Notstromversorgung der dafür notwendigen Informations- und Kommunikationssysteme weiter garantiert werden können. Bei allen Kreditinstituten sind die kritischen Server (mit Daten zu Zahlungsverkehr, Anlageverwaltung u. Ä.) gegen Stromausfall gesichert, sodass essenzielle Daten nicht verloren gehen.

Größere Banken verfügen zudem über eine ausreichende Notstrom-

versorgung, um auch die Arbeitsplätze (Backoffice, Schalter) der Angestellten zu versorgen. Diese können zunächst wie gewohnt weiterarbeiten. Bei kleineren Banken, die nicht über entsprechende Vorkehrungen verfügen, kann hingegen ein Großteil der Angestellten nicht mehr weiterarbeiten. Da zunächst nicht bekannt ist, wie lange der Stromausfall dauern wird, bleiben die Angestellten vorerst im Gebäude (EBP 2010, S. 45 ff.).

Die Schalter sind zunächst noch besetzt, und die Kundschaft wird weiter bedient. Bargeld ist genügend vorhanden. Noch erreichen Bargeldtransporte, die zum Zeitpunkt des Stromausfalls unterwegs waren, ihren Bestimmungsort, wenn auch mit Verspätungen aufgrund aufkommender Verkehrsprobleme wie Staus und Sperrungen (Kap. III.2.2). Bei einigen kleineren Banken sind keine Vorkehrungen für den Weiterbetrieb der Schalter getroffen, diese müssen ihre Schalter schließen.

Die reine Verwaltung von Publikumseinlagen und von (Finanz-) Anlagen ist zu Beginn des Stromausfalls nicht tangiert, sofern die betreffende Bank die entsprechenden Arbeitsplätze im Backoffice mit Notstrom versorgen kann. Die Daten sind gesichert, und Aufträge, die vor dem Stromausfall an die entsprechende Handelsplattform abgeschickt wurden, können noch ausgeführt werden. Auch Kredite können nach Beginn des Stromausfalls noch vergeben werden.

Die Bevölkerung hat in großen Teilen des betroffenen Gebiets keine Möglichkeit mehr, Geld an Geldautomaten abzuheben oder einzuzahlen. Diese verfügen in der Regel weder über eine USV noch eine Netzersatzanlage und sind demnach gleich zu Beginn außer Betrieb. Dies gilt nicht für Automaten, die direkt an Bankgebäuden angebracht und an die dortige interne Netzersatzanlage angeschlossen sind. Die Zahl dieser Geldautomaten ist allerdings sehr klein (EBP 2010, S. 46). In der Folge stehen die Kunden an den Schaltern ihrer Banken an, um Bargeld abzuheben, da mittlerweile ersichtlich geworden ist, dass auch die elektronische Bezahlung mit Debit- oder Kreditkarten in den Geschäften nicht mehr möglich ist.

Lohnzahlungen, die ein Arbeitgeber schon in Auftrag gegeben hat und für die bei der entsprechenden Bank Deckung besteht, werden

noch ausgeführt. Lohnzahlungen neu in Auftrag zu geben, ist teilweise schon schwierig: Bei vielen kleineren und mittleren Unternehmen sind die Informations- und Kommunikationsinfrastrukturen ausgefallen (EBP 2010, S. 47).

Zwei bis acht Stunden

Der Betrieb in größeren Banken bleibt im Wesentlichen aufrechterhalten. Insbesondere die kritischen Geschäftsprozesse sind sichergestellt. Allerdings macht sich in einigen Bereichen nun bemerkbar, dass Kommunikationsanlagen, die auf dem öffentlichen Telefonnetz basieren, nach und nach ausfallen.

Die Schalter bleiben besetzt, und es wird, falls möglich und gemäß BCM vorgesehen, noch bedient. Es ist schon deutlich mehr Kundschaft an den Schaltern, die Geld von ihrem Konto abheben möchte, da die Geldautomaten nicht mehr funktionieren. Bargeld ist genügend vorrätig; auch werden noch Bargeldtransporte durchgeführt. Bei einigen kleineren Banken sind die USV ausgefallen oder die Schalter sind von vornherein geschlossen. Es kommt gelegentlich zu Unmutsäußerungen seitens der Kundschaft. Einige Vorgänge werden angesichts der unklaren Situation zunächst schriftlich auf Papier festgehalten, um diese später zu verbuchen (EBP 2010, S. 47).

Während ein Teil der Angestellten (insbesondere im Backoffice von kleineren Banken) nachhause geschickt wird, müssen andere am Arbeitsplatz bleiben. Sie werden vor allem an den Schaltern eingesetzt, um die allmählich zahlreicher werdende Kundschaft soweit möglich zu bedienen. Insbesondere die Ausgabe von Bargeld ist vermehrt nachgefragt, aber auch besorgte Fragen nach Lohnzahlungen, Überweisungen und Ähnliches müssen beantwortet werden. **In Banken, in denen das Personal zu wenig vorbereitet ist und/oder die Ausgabe von Bargeld nicht richtig funktioniert, spielen sich teils chaotische Szenen ab. An einigen Orten ist der Einsatz von Polizeikräften notwendig.** Diese Banken entscheiden, früher zu schließen und – in der Annahme, dass der Strom dann wieder da ist – am nächsten Tag die (unerledigten) Geschäfte wieder aufzunehmen (EBP 2010, S. 47 f.).

Spätestens acht Stunden nach Beginn des Stromausfalls wird das Tagesgeschäft soweit möglich abgeschlossen. Informationen über die absehbare Dauer des Stromausfalls fehlen. Dennoch machen sich in einigen größeren Banken die Geschäftsleitung und die Verantwortlichen des BCM erste Gedanken über nächste Schritte im Fall eines länger andauernden Stromausfalls. Es wird geprüft, ob kritische Geschäftsprozesse in nichtbetroffene Landesteile oder sogar in das Ausland verlegt werden sollen. Zudem müssen bei größeren Banken einige Angestellte über Nacht im Gebäude bleiben, um sicherzustellen, dass die kritischen Geschäftsprozesse auch am nächsten Tag weitergeführt werden können, wenn bis dahin Strom immer noch nicht verfügbar sein sollte (EBP 2010, S. 48).

Die Verwaltung der Publikumseinlagen und der Anlagen ruht dort, wo die Banken ihren Angestellten keine notstromversorgten Arbeitsplätze zur Verfügung stellen können. Dies ist insbesondere bei den kleineren Banken der Fall. Größere Institute verwalten in ihren wichtigsten Filialen wie gewohnt bis zum Ende des Arbeitstages und überführen – sofern möglich – die Verwaltung der Publikumseinlagen und der Finanzanlagen über ihre gegen Stromausfall gesicherten Datenleitungen in nichtbetroffene Filialen.

Die Kunden im betroffenen Gebiet haben zunehmend Schwierigkeiten, mit ihren Banken zu kommunizieren. Sowohl Anweisungen über Telefon (mobil und Festnetz) als auch über das Internet sind zum großen Teil nicht mehr möglich. In der Folge erleiden Investoren und Unternehmen wirtschaftliche Verluste aufgrund entgangener Gewinne (EBP 2010, S. 48). Kreditverhandlungen werden zunehmend weniger geführt, sofern sich die Beteiligten trotz des Verkehrschaos überhaupt treffen können. Überweisungen von Konto zu Konto innerhalb des Bankensektors funktionieren noch. Verhandlungen über Telefon sind bereits wenige Stunden nach Beginn des Stromausfalls nicht mehr möglich.

Acht bis 24 Stunden

Auch am Tag nach dem Stromausfall bleibt der Betrieb der kritischen Geschäftsprozesse in den größeren Banken im Wesentlichen

aufrechterhalten. Allerdings verschlechtern sich die Arbeitsbedingungen, da in den meisten Banken beispielsweise die Kantinen nicht mehr betrieben werden können, Aufzüge nicht funktionieren und Heizungen ausgefallen sind. Beleuchtung und Arbeitsplätze sind nach wie vor verfügbar. Etwa zwei Drittel der Angestellten, die zum Erscheinen verpflichtet sind, erscheinen an ihren Arbeitsplätzen (EBP 2010, S. 19). Zusammen mit den Teams, die über Nacht im Gebäude geblieben sind, müssen sie die kritischen Geschäftsprozesse aufrechterhalten und z. T. die Schalter besetzen. Kommuniziert werden kann nun nur noch über die gesicherten Datenleitungen (Zahlungsverkehrssysteme, Verbindungen zu Clearingorganisationen und Handelsplätzen, Verbindungen zu anderen größeren Banken) (EBP 2010, S. 49).

Die Schalter sind in größeren Banken besetzt, und Bargeld kann weiterhin ausgegeben werden. Auch werden noch Geldtransporte durchgeführt. Immer mehr Menschen möchten Bargeld abheben, da nur noch mit Bargeld eingekauft werden kann. Auch Fragen zu Lohnzahlungen und Rechnungen müssen beantwortet werden. Kleinere Banken öffnen erst gar nicht und betreiben nur noch das Backoffice bzw. die kritischen Geschäftsprozesse (EBP 2010, S. 49).

Die Verwaltung der Publikumseinlagen und der Finanzanlagen ruht nunmehr vor allem bei kleineren Banken, wo keine notstromversorgten Arbeitsplätze verfügbar sind. Größere Institute verwalten weiter, allerdings mit allen resultierenden Einschränkungen (verschlechterte Arbeitsbedingungen, kaum/keinen Kontakt zu Kunden/Investoren). Sie leiten aber erste Schritte ein, um diese Tätigkeiten in nichtbetroffene Gebiete auszulagern.

Investoren und Unternehmen im betroffenen Gebiet haben nun fast keine Möglichkeiten mehr, mit ihren Banken zu kommunizieren. Sowohl Anweisungen über Telefon (mobil und Festnetz) als auch über das Internet sind nicht mehr möglich, auch wenn die betreffenden Investoren/Unternehmen über funktionierende Endgeräte verfügen sollten. In der Folge erleiden sie wirtschaftliche Verluste. Verhandlungen über Kreditvergaben werden nur noch in äußerst dringenden Fällen durchgeführt.

Da nach wie vor davon ausgegangen wird, dass die Stromversorgung bald wiederhergestellt wird, und vielerorts die Tragweite des Ereignisses noch nicht bekannt ist, werden von den Geschäftsleitungen und den Verantwortlichen des BCM erst am Ende des Tages nach dem Stromausfall die ersten Schritte für den Fall eines länger dauernden Stromausfalls eingeleitet (wie kritische Geschäftsprozesse in nichtbetroffene Regionen verlegen) (EBP 2010, S. 50).

24 Stunden bis eine Woche

In der Woche nach dem Stromausfall bleibt in den größeren Bankhäusern weiterhin ein eingeschränkter Betrieb (d. h. Aufrechterhaltung der kritischen Geschäftsprozesse sowie – eingeschränkt – Bedienung an den Schaltern) möglich. Gegen Ende der ersten Woche sind die kritischen Geschäftsprozesse in nichtbetroffene Regionen ausgelagert. Dazu wurden die dafür notwendigen Arbeitskräfte mit Bussen aus nichtbetroffenen Gebieten zu den für solche Fälle vorgehaltenen Ausweichstandorten transportiert. Dort realisieren sie die kritischen Geschäftsprozesse mittels der von einem vorausgeschickten Team in Betrieb genommenen redundanten Informations- und Kommunikationsinfrastrukturen. Allerdings müssen zusätzlich aus nichtbetroffenen Regionen weitere Arbeitskräfte hinzugezogen werden, da nicht alle erforderlichen Angestellten bereit waren, ihre Familien und ihren Wohnraum im betroffenen Gebiet zurückzulassen (EBP 2010, S. 51).

Auszahlungen von Bargeld an den Schaltern sind nach einigen Tagen praktisch nicht mehr möglich, da insbesondere die Geldtransporte durch Private von den Bundesbankfilialen zu ihren Bestimmungsorten nicht mehr in der notwendigen Anzahl durchgeführt werden. Zwar werden die für eine solche Situation vorgesehenen Maßnahmen (Verteilung der Geldnoten unabhängig von privat durchgeführten Geldtransporten) durch die Bundesbank in Angriff genommen, nachdem absehbar geworden ist, dass der Stromausfall längere Zeit dauert. Sie wird dabei von weiteren staatlichen Stellen (wie der Polizei) unterstützt (BBK 2008a, S. 119). Doch angesichts der Größe des betroffenen Gebiets bleibt Bargeld knapp. Verschärfend kommt hinzu, dass aufgrund von Transportproblemen und Hamsterkäufen die Preise für

Grundnahrungsmittel und andere Güter steigen. Die Bevölkerung ist mittlerweile stark verunsichert, da zunehmend klarer wird, dass der Stromausfall weiter andauern wird (EBP 2010, S. 51 ff.).

Am Ende der ersten Woche haben nun auch die größeren Banken Probleme, ihre Notstromversorgung aufrechtzuerhalten. Die Treibstoffvorräte für die Netzersatzanlagen gehen zur Neige, und es gibt Probleme bei Nachschublieferungen. In der Folge werden die meisten Schalter geschlossen. Kritische Geschäftsprozesse sind davon nicht tangiert, da diese in nichtbetroffene Regionen ausgelagert wurden. Kleinere Banken stellen ihre kritischen Geschäftsprozesse ein und versuchen, Datenverluste zu vermeiden (EBP 2010, S. 52). Die Verwaltung der Publikumseinlagen und der Finanzanlagen wurde entweder in nichtbetroffene Regionen ausgelagert oder ruht.

Unternehmen, die ihre Tätigkeiten nicht in nichtbetroffene Regionen verlegt haben oder deren (kleinere) Banken nicht über die Möglichkeit verfügen, mittels Ausweichinfrastruktur die Verwaltung der Finanzanlagen weiterzuführen, haben nun keine Möglichkeit mehr, zu investieren und zu finanzieren. Sie erleiden deshalb größere wirtschaftliche Verluste. Verhandlungen über Kreditvergaben sowie Kreditvergaben selbst sind – innerhalb des betroffenen Gebiets – vollständig zum Erliegen gekommen.

Bei ersten Betrieben treten gegen Ende der Woche Liquiditätsengpässe auf, da einerseits keine Einnahmen mehr getätigt werden können oder Rechnungen aufgrund des Stromausfalls von den jeweiligen Kunden nicht bezahlt werden und andererseits zahlreiche Außenstände dennoch beglichen werden (automatisierte Zahlungen werden von den Banken trotz Stromausfall ausgeführt) (EBP 2010, S. 53).

Ein Blick in Woche 2

Die kritischen Geschäftsprozesse der größeren Banken bleiben dank der Ausweichstandorte weiter gewährleistet. Nachdem zu Anfang ein Personalengpass für den Betrieb der Ausweichstandorte existierte, ist dieser nun mittels Arbeitskräften aus nichtbetroffenen Regionen behoben worden.

In den Hauptfilialen einiger Banken bestehen zwar Planungen, zu bestimmten Zeiten zu öffnen und eine begrenzte Zahl von Schaltern zu besetzen, allerdings haben die meisten Verantwortlichen in der zweiten Woche entschieden, die Schalter zu schließen. Gründe sind mangelnde Sicherheit für das Personal (unzufriedene und z. T. aggressive Kundschaft), **Mangel an Bargeld**, gefährdete Versorgung mit Notstrom sowie die Tatsache, dass sehr viele Angestellte ihren Arbeitsplätzen fernbleiben, um sich um ihre Familien und Wohnungen zu kümmern. Banken, die in Schließfächern Wertsachen einlagern, sind einem erhöhten Einbruchsrisiko ausgesetzt und müssen ggf. von privaten Sicherheitsfirmen oder von der Polizei bewacht werden.

Die Bargeldversorgung der Bevölkerung wird durch Maßnahmen der Bundesbank nur mühsam aufrechterhalten.

Investoren und Unternehmen, die ihre Tätigkeiten nicht verlegen konnten oder nicht über die Möglichkeit einer Ausweichinfrastruktur verfügen, haben nun keine Möglichkeit mehr, zu investieren und zu finanzieren und erleiden wirtschaftliche Verluste. Bei einer Vielzahl an Unternehmen, deren Verpflichtungen trotz des Stromausfalls weiterlaufen, treten Liquiditätsengpässe auf.

ZAHLUNGS- UND DATENVERKEHRSSYSTEM 2.6.3.2

Wie zuvor gezeigt, ist das Zahlungs- und Datenverkehrssystem zwischen den Finanzintermediären (Banken und bankähnliche Organisationen), den Handelsplattformen und den Zentralbanken gegen einen großflächigen und langandauernden Stromausfall weitgehend gesichert.

Nicht gesichert ist dagegen der (elektronische) Zahlungs- und Datenverkehr zwischen dem Zahlungsempfänger bzw. dem Zahlungsleistenden und deren jeweiligem Zahlungsintermediär. Bei einem Stromausfall wird es in vielen Geschäften umgehend nicht mehr möglich sein, mit einer Debit- oder einer Kreditkarte zu zahlen, da die Endgeräte nicht mehr funktionieren. Dort, wo ein Geschäft über eine USV verfügt, dürften elektronische Zahlungen noch so lange erfolgen, wie die Leitungen des Festnetztelefons funktionieren (etwa bis zu acht Stunden).

Null bis zwei Stunden

Nach dem Ausfall der Stromversorgung stellen sowohl bei Zahlungsintermediären als auch bei den entsprechenden Clearingorganisationen zunächst die USV und später die Netzersatzanlagen die Funktion der Systeme sicher. Hierdurch wird der Verlust der Daten für den elektronischen Zahlungsverkehr verhindert. Auch die Kommunikationsinfrastrukturen (gesicherte Datenleitungen) funktionieren, sodass der (automatisierte) Austausch zwischen den Zahlungsintermediären, Clearingorganisationen und Zentralbanken über die gesamte Dauer des Stromausfalls weiter stattfinden kann (EBP 2010, S. 62).

Auch die Tätigkeiten der Europäischen Zentralbank und der Deutschen Bundesbank sind nicht eingeschränkt, da auch diese gegen einen Stromausfall gesichert sind. Das gesamteuropäische Zahlungsverkehrssystem ist vom Stromausfall grundsätzlich nicht betroffen und funktioniert über die gesamte Dauer des Stromausfalls.

Probleme gibt es allerdings bei den Zahlungsleistenden und den Zahlungsempfängern: In vielen Geschäften ist es bereits unmittelbar nach dem Stromausfall nicht mehr möglich, elektronische Zahlungen mit Debit- und Kreditkarten durchzuführen, da die entsprechenden Terminals (Einlesegeräte) nicht mehr funktionieren. Dadurch können sowohl die Karten nicht mehr eingelesen als auch keine entsprechenden Zahlungsanweisungen an die Zahlungsintermediäre geschickt werden. Käufe können nur noch mit Bargeld durchgeführt werden. Aber auch Anweisungen für Distanzzahlungen (von zuhause mit dem Internet) sind nicht mehr möglich, da die Zahlungsleistenden in den meisten Fällen keine Möglichkeit mehr haben, ihre Computer zu benutzen und entsprechende Anweisungen zu geben. Größere Unternehmen, die sich auf einen Stromausfall vorbereitet und für ihre Rechner eine USV installiert haben, haben in dieser Phase noch die Möglichkeit, Zahlungsanweisungen an Banken zu übermitteln oder Bestätigungen zu empfangen.

Zwei bis acht Stunden

In den Geschäften sind nur noch Barzahlungen möglich. In den ersten Stunden, nachdem die Menschen den Stromausfall zur Kenntnis

genommen und akzeptiert haben, stellt dieser Ausfall des elektronischen Zahlungsverkehrs noch kein großes Problem dar. Viele gehen davon aus, dass der Strom in einigen Stunden wieder da sein wird und verschieben ihre Besorgungen. Andere heben bei ihren Banken Geld ab, was noch weitgehend problemlos möglich ist. Privatpersonen verschieben ihre Zahlungsanweisungen, die sie über das Internet machen wollten, auf später, ebenfalls in der Annahme, dass der Strom bald wieder da sein wird. Größere Unternehmen, die sich auf einen Stromausfall vorbereitet haben, übermitteln ihre Zahlungsanweisungen so lange, wie die Kommunikationsleitungen, auf denen das Internet basiert, noch funktionieren.

Acht bis 24 Stunden

Einige Geschäfte haben trotz des Stromausfalls geöffnet und bieten z. T. reduzierte Sortimente gegen Barzahlung an. Viele Menschen gehen nach wie vor davon aus, dass der Strom in den nächsten Stunden wieder da sein wird. Aus diesem Grund werden Einkäufe auf später verschoben. Andere heben mangels funktionierender Geldautomaten in den Banken ab. Kleinere Banken schließen allerdings. Nun können auch größere Unternehmen keine Zahlungsanweisungen mehr durchführen. Zudem arbeiten jetzt – wenn überhaupt – die meisten Betriebe nur noch eingeschränkt, viele haben sogar ganz geschlossen.

24 Stunden bis eine Woche

In den ersten Tagen ist die Bargeldversorgung der Bevölkerung an den geöffneten Schaltern der Banken noch möglich; auch ist die Nachfrage nach Bargeld noch moderat, da die meisten Menschen von einem baldigen Ende des Stromausfalls ausgehen. Besorgungen werden auf später verschoben.

Sobald kommuniziert wird, dass ein Ende des Stromausfalls nicht absehbar ist, steigt nicht zuletzt aufgrund mangelnder Bezahlmöglichkeiten in der Bevölkerung die Sorge vor Versorgungsengpässen. In einigen Banken und Einzelhandelsgeschäften spielen sich teilweise chaotische Szenen ab, da die Menschen versuchen, an Bargeld oder an Güter des täglichen Gebrauchs zu gelangen. Die Situation verschärft

sich, da einige Lieferanten die Geschäfte nicht mehr beliefern (können) – teils aus Mangel an Transportmöglichkeiten, teils aus Furcht, dass die Lieferungen unbezahlt bleiben. Diebstähle und Plünderungen treten vereinzelt auf (EBP 2010, S. 64).

Ein Blick in Woche 2

Die von der Bundesbank ergriffenen Maßnahmen zur Versorgung der Bevölkerung mit Bargeld greifen nur bedingt, da die Geschäfte leer geräumt sind und die Preise besonders nachgefragter Güter in die Höhe schnellen. Zudem nimmt die Zahl der mobilen Händler zu, die Güter des alltäglichen Bedarfs zu stark überhöhten Preisen verkaufen. Personen, die Bargeld vorrätig hatten oder über die Maßnahmen der Bundesbank zu Bargeld gekommen sind, nutzen dieses, um bei Bauern und anderen Nahrungsmittellieferanten (z. T. Schwarzmarkthändler) einzukaufen. Der Tausch von Wertgegenständen gegen Gebrauchsgüter und Lebensmittel bleibt eher die Ausnahme (EBP 2010, S. 65).

FAZIT 2.6.4 BANKDIENSTLEISTUNGEN 2.6.4.1

Sämtliche kritischen Geschäftsprozesse sind in diesem Teilsektor durch USV bzw. eine über längere Zeit hinweg funktionierende Netzersatzanlage gewährleistet. Diese hält in der Regel so lange vor, dass die kritischen Geschäftsprozesse in ein nichtbetroffenes Gebiet ausgelagert werden können.

Gemäß BCM werden sofort nach dem Stromausfall die entsprechenden Teams eingesetzt, um die Aufrechterhaltung der kritischen Geschäftsprozesse zu gewährleisten. Teilweise müssen Angestellte deshalb über Nacht im Gebäude verbleiben. Spätestens wenn nach zwei Tagen das Ausmaß des Ausfalls deutlich wird, werden Maßnahmen zur Auslagerung bzw. zur längerfristigen Sicherstellung der kritischen Geschäftsprozesse umgesetzt. Der Daten- und Zahlungsverkehr, die Datenhaltung und weitere kritische Geschäftsprozesse sind deshalb über die ganze Zeit des Stromausfalls hinweg sichergestellt. Banken, die in Schließfächern Wertsachen eingelagert haben, müssen besondere Maßnahmen zur Sicherung ergreifen. Auch für die (Not-) Bargeldversorgung werden Schritte unternommen, wozu ebenfalls der Einsatz von Polizeikräften notwendig ist.

Das Weiterarbeiten der Angestellten ist in begrenztem Umfang bis zu einer Woche möglich, und die Schalter in größeren Banken können besetzt werden. Die Angestellten haben aber unter verschlechterten Arbeitsbedingungen zu leiden. Spätestens nach einer Woche muss der Betrieb nach und nach überall eingestellt werden. Schäden an den Bankgebäuden sind keine zu erwarten, außer, wenn in einzelnen Filialen dringend erforderliche Reparatur- und Instandsetzungsarbeiten nicht mehr vorgenommen werden (z. B. aufgrund von Frostschäden). Nach und nach fallen die Kommunikationsverbindungen zwischen den Banken und den Kunden aus. Bereits nach wenigen Stunden, wenn sowohl Mobil- als auch Festnetztelefonie nicht mehr nutzbar sind, können Kunden nur noch physisch mit der Bank in Verbindung treten. **Die Bargeldausgabe über Automaten fällt sofort bei Beginn des Stromausfalls aus und wird über die ganze Dauer nicht wieder hergestellt (auch elektronische Zahlungen in Geschäften sind nicht mehr möglich). Damit droht die Bargeldversorgung der Bevölkerung zusammenzubrechen. Da beim Einkauf auch nicht mehr bargeldlos bezahlt werden kann, wachsen Unsicherheit und Aggression in der Bevölkerung.**

ZAHLUNGS- UND DATENVERKEHR

Der Zahlungsverkehr zwischen Banken, Clearingorganisationen und Zentralbanken ist dank technischer Maßnahmen (Notstromversorgung) über die ganze Dauer des Stromausfalls gewährleistet. Vorbereitete Notfallpläne werden umgesetzt. Ausgewähltes Bankpersonal in Banken hält kritische Geschäftsprozesse aufrecht. Dies bedeutet für die eingesetzten personellen Ressourcen der Banken eine große Belastung.

In Geschäften, die mit USV und/oder Netzersatzanlagen ausgerüstet sind, ist die elektronische Bezahlung noch für die ersten Stunden möglich. Sobald aber die Festnetztelefonverbindungen ausfallen, ist dies nicht mehr möglich. In anderen Geschäften bleibt nur die Bezahlung mit Bargeld.

Ein großflächiger Stromausfall beeinträchtigt das Bankdienstleistungssystem an sich also nur begrenzt. Insbesondere größere Banken

können in der Regel die Publikumseinlagen über die gesamte Dauer des Stromausfalls bewirtschaften sowie ihre Verbindungen mit Clearingorganisationen, der Zentralbank und den Börsenplätzen aufrechterhalten. Möglich ist dies dank Notstromversorgung und aufgrund der Auslagerung kritischer Geschäftsprozesse in nichtbetroffene Regionen. Auch der elektronische Zahlungs- und Datenverkehr zwischen den Banken, Clearingorganisationen und Handelsplätzen ist gegen einen länger dauernden Stromausfall gesichert und kann weiter erfolgen. Ebenso ist der Betrieb der Handelsplätze, namentlich der Hauptbörse in Frankfurt, auch bei einem länger dauernden Stromausfall gesichert, und die Handelstätigkeiten sind grundsätzlich nicht beeinträchtigt. Ausnahmen bilden allenfalls Regionalbörsen (EBP 2010, S. 78).

Als Achillesferse erweisen sich dagegen die unterbrochenen Kommunikationswege zwischen den Banken, Clearingorganisationen und Handelsplätzen einerseits und den Personen und Unternehmen, die Finanzdienstleistungen nachfragen, andererseits. Deshalb können Finanzdienstleistungen von den Nachfragern größtenteils nicht mehr in Anspruch genommen werden. **Nach einer gewissen Zeit sind also Bargeldauszahlungen, Lohnüberweisungen, Kreditaufnahme oder Ähnliches, aber auch Kartenzahlungen nicht mehr möglich.**

VERLETZBARKEIT, BEWÄLTIGUNGSOPTIONEN UND HANDLUNGSBEDARF – SCHLUSSFOLGERUNGEN

221: **Während der Zahlungs- und Datenverkehr der Banken und die Handelsaktivitäten an der Börse trotz des Stromausfalls relativ robust erscheinen, sind die Bankdienstleistungen für die Kunden aufgrund der ausgefallenen Kommunikationswege bald vom Zusammenbruch bedroht.**

VERLETZBARKEIT UND BEWÄLTIGUNGSKAPAZITÄTEN

Die Kunden könnten keine Geschäfte mit der Bank via Telefon oder Internet tätigen. Bargeldauszahlungen an Automaten erfolgen nicht mehr; ebenso wenig kann der Kunde in Geschäften bargeldlos bezahlen. Die Nachfrage nach Bargeld dürfte deshalb schnell zunehmen,

auch weil ein Bürger in Deutschland durchschnittlich nur 118 Euro mit sich tragen soll (Deutsche Bundesbank 2009b, S. 40). Der sofortige Ausfall der Bargeldversorgung über Geldautomaten und später auch an den Schaltern der Banken sowie der Zusammenbruch der bargeldlosen Bezahlung führen in Geschäften und Banken nach einer Phase der Gelassenheit mit der Zeit zu Unmutsäußerungen und teils zu aggressiven Auseinandersetzungen. Sobald klar ist, dass der Stromausfall noch lange andauern wird, verstärkt sich die Unsicherheit in der Bevölkerung. **Die Menschen haben Angst, sich nicht mehr mit Nahrungsmitteln und anderen Gütern des täglichen Bedarfs versorgen zu können, da sie über kein Bargeld und keine bargeldlosen Zahlungsmöglichkeiten mehr verfügen. In der Folge kommt es zu z. T. gewaltsamen Auseinandersetzungen, Diebstahl und Einbruch. Zeitweise muss die Polizei eingreifen. Zudem wird mit zunehmender Dauer des Stromausfalls die Bewachung einzelner Geschäfte notwendig.** Der Umsatz in den Geschäften bricht ein. Es ist auch nicht auszuschließen, dass die Preise für Güter des alltäglichen Bedarfs bereits im Verlauf der ersten Woche steigen. Die Information der Kunden und eine angemessene Risikokommunikation in Abstimmung mit den Katastrophenschutzbehörden werden deshalb immer wichtiger.

In den Fokus rückt die Bargeldversorgung der Bevölkerung. Der Deutschen Bundesbank zufolge sind zur »Bewältigung eines Not- oder Katastrophenfalls ... spezielle Vorkehrungen im Rahmen einer Krisenmanagementorganisation« getroffen worden (BBK 2008a, S. 120). Ob aber in einem großen Gebiet kontinuierlich und über längere Zeit Bargeld bedarfsgerecht durch private Wertdienstleister transportiert, verteilt und durch die Banken ausgegeben werden kann, dies scheint doch zweifelhaft.

Die Wirtschaft nimmt aufgrund weitgehend fehlender Möglichkeiten für die Bevölkerung und die Unternehmen, bargeldlos einzukaufen, Kreditverhandlungen durchzuführen, Lohnzahlungen zu tätigen, Börsenaufträge zu erteilen sowie wegen bald auftretender Liquiditätsengpässe Schaden.

INFORMATIONSBEDARF, HANDLUNGSPERSPEKTIVEN

Als besonderer Schwachpunkt hat sich in den Folgenanalysen die Bargeldversorgung der Bevölkerung erwiesen. Deshalb steht insbesondere die Deutsche Bundesbank vor der Aufgabe, in Zusammenarbeit mit anderen Organisationen und Einsatzkräften des Bevölkerungsschutzes sowie den Banken, die Bargeldversorgung der Bevölkerung zumindest rudimentär sicherstellen (EBP 2010, S. 79). Um hierfür bessere Voraussetzungen zu schaffen, wäre zu prüfen, ob die Bundesbank in den Kreis der Bevorrechtigten für die Anforderung von Transportkapazitäten gemäß VerkLG aufgenommen werden sollte. Für den Katastrophenfall müsste wahrscheinlich ein erweitertes Logistik- und Sicherheitskonzept zum Tragen kommen, da beispielsweise nicht zu erkennen ist, ob und wie die privaten Dienstleister die intensivierte Auslieferung von Bargeld ausreichend absichern könnten.

Geplant ist die Schließung von zahlreichen Filialen der Deutschen Bundesbank in den nächsten Jahren. Es wäre zu reflektieren, ob und inwiefern diese Einschnitte in die Infrastruktur Auswirkungen auf die Bargeldversorgung im Katastrophenfall hätten.