bankenverband

Online- und Mobile Banking: **sicher über Browser und App**

Vorwort

Online- und Mobile Banking machen die Erledigung von Bankgeschäften schnell und komfortabel. Doch was ist zu berücksichtigen und welche Verhaltensregeln müssen Sie als Nutzer befolgen, um Ihre Bankgeschäfte sicher zu erledigen? Wie funktioniert sicheres Online- und Mobile Banking? In dieser Broschüre zeigen wir Ihnen anhand von ausgewählten Anwendungsfällen, worauf Sie beim Online- und Mobile Banking achten sollten.

Inhalt

Banking – **zu Hause und unterwegs**

Ganz gleich, ob Überweisungen, Buchungen vom Sparbuch, Wertpapierorders und sogar Kreditanträge – alltägliche Bankgeschäfte lassen sich heute schnell und unabhängig von den Öffnungszeiten der Bankfiliale tätigen: entweder von zu Hause ganz klassisch über den Browser am PC oder unterwegs per Smartphone oder Tablet über Banking-Apps. Tätigen Sie Ihre Bankgeschäfte über ein stationäres Gerät, spricht man vom „Onlinebanking“. Greifen Sie lieber auf ein mobiles Endgerät zurück, spricht man hingegen vom „Mobile Banking“.

Bankgeschäfte auf eigenen Geräten

Für die Sicherheit des Online- und Mobile Banking trifft Ihre Bank umfangreiche Maßnahmen: Dazu gehört unter anderem die Verschlüsselung vertraulicher Daten. Zudem werden Zahlungsaufträge auf verdächtige Transaktionen hin überprüft. Auf die Sicherheit der von Ihnen genutzten Hard- und Software hat Ihre Bank jedoch keinen Einfluss. Daher ist es wichtig, dass Sie

Vorkehrungen zum Schutz Ihrer Geräte wie PC, Smartphone oder Tablet sowie des Browsers treffen und einige Sorgfaltspflichten beachten. Welche das im Detail sind, können Sie in den Online- und Mobile-Banking-Bedingungen Ihrer Bank nachlesen.

Grundsätzlich sollten Sie für Ihre Bankgeschäfte nur eigene Geräte verwenden. Wenn Sie ein Gerät nicht kennen, wie zum Beispiel den PC oder das Tablet eines Bekannten, haben Sie keine Informationen über den „Gesundheitszustand" des betreffenden Geräts. Ist es beispielsweise mit einer Schadsoftware infiziert, könnten Ihre Tastatureingaben oder Bildschirminhalte unbemerkt aufgezeichnet und an Dritte weitergeleitet werden.

Apps nur aus autorisierten App-Stores

Wenn Sie Bankgeschäfte auf Ihrem Smartphone oder Tablet erledigen wollen, können Sie hierfür eine Banking-App Ihrer Bank verwenden. Laden Sie diese ausschließlich aus dem offiziellen App-Store herunter. Folgen Sie keinen Angeboten zum Download aus anderen Quellen, wie E-Mails oder Webseiten.

Tipps

Onlinebanking nicht auf fremden Geräten

Banking-App aus offiziellem App-Store laden

Ins Online- und Mobile Banking **starten**

Der Start ins Onlinebanking erfolgt in der Regel über die Website Ihrer Bank. Geben Sie die Adresse am besten händisch ein. Nutzen Sie keine Links, die Ihnen beispielsweise per E-Mail oder SMS übersandt wurden. Die drohende Gefahr hinter diesen Links: Kriminelle versuchen oft über gefälschte Websites Ihre sensiblen Daten, wie beispielsweise Ihre Zugangsdaten zum Onlinebanking, Ihr Geburtsdatum oder Ihre Adresse, auszuspähen, um diese für betrügerische Zwecke zu missbrauchen.

Adressleiste im Blick

Achten Sie darauf, wie die Internetadresse Ihrer Bank im Browser angezeigt wird: Die Adresse sollte stets mit „https“ beginnen. Damit wird angezeigt, dass es sich um eine sogenannte SSL/TLS-Verbindung handelt, die für die Dauer Ihrer Onlinebanking-Sitzung dafür sorgt, dass die Daten zwischen Ihrem Browser und dem Banksystem verschlüsselt übertragen werden. Häufig wird

stattdessen auch ein Schlüssel- bzw. Schlosssymbol in der Adressleiste angezeigt: Auch dieses Symbol muss während der gesamten Sitzung zu sehen sein. Fehlt die Anzeige von „https“ oder das Schlüssel- bzw. Schlosssymbol in der Adressleiste oder erscheint Ihnen die Internetseite Ihrer Bank nicht vertraut, brechen Sie den gesamten Vorgang ab.

Schutz der Anmeldedaten

Für die Anmeldung zum Onlinebanking fragt Ihre Bank Sie stets nach Zugangsdaten, um Sie sicher zu identifizieren. Diese können beispielsweise eine Persönliche Identifikationsnummer (PIN) oder ein Passwort in Kombination mit Ihrer Teilnehmernummer sein. Achten Sie darauf, dass Sie ein sicheres Passwort verwenden. In Banking-Apps können für die Anmeldung auch biometrische Merkmale genutzt werden.

Unterschiede gibt es, wenn für den Zugriff zusätzlich eine Transaktionsnummer (TAN) gefordert wird: Bei einigen Banken muss die TAN jedes Mal eingegeben werden, andere Banken bitten Sie hingegen nur alle 90 Tage, eine TAN bei der Anmeldung einzugeben. In jedem Fall gilt: Schützen Sie Ihre Zugangsdaten, die TAN sowie die für den TAN-Empfang erforderlichen Geräte vor unberechtigtem Zugriff.

Betrüger versuchen immer wieder, über Telefonate oder E-Mail-Kommunikation an Zugangsdaten und TAN zu gelangen. Gut zu wissen: Ihre Bank wird Sie niemals kontaktieren, um nach diesen Daten zu fragen. Gehen Sie auf keinen Fall darauf ein, auch wenn Ihnen der angebliche Bankmitarbeiter mit einer Kontosperre oder anderen Konsequenzen droht. Ihre Bank fordert Sie auch niemals zur Eingabe mehrerer TAN, der PIN oder weiterer persönlicher Daten auf. Brechen Sie den Vorgang sofort ab und melden Sie den Vorfall umgehend Ihrer Bank.

Tipps

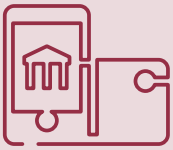
Onlinebanking-Adresse händisch eingeben

„https“ oder Schlüssel- bzw. Schlosssymbol sichtbar?

PIN, TAN und Geräte schützen

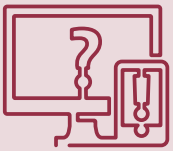
Auf einen Blick: **die TAN-Verfahren**

Um einen Auftrag, zum Beispiel eine Überweisung, zu erteilen, müssen Sie diesen mit einer Transaktionsnummer (TAN) freigeben. Diese TAN ist an die betreffende Transaktion gebunden und dient quasi als Signatur, durch die der Auftrag autorisiert wird. Ihre Bank bietet Ihnen meist mehrere Verfahren an. Sie können wählen, ob Sie die TAN über Ihr Smartphone, Tablet, Handy mit SIM-Karte oder über den TAN-Generator generieren wollen. TAN können auf unterschiedliche Weise empfangen oder erzeugt werden, zum Beispiel per …



… App auf Smartphone und Tablet

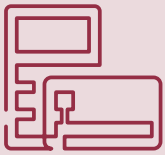
Um App-basierte Verfahren zu nutzen, müssen Sie eine TAN-App, eine gesicherte-Software zum Empfang einer TAN, auf Ihrem Mobilgerät installieren. Je nach Art der technischen Umsetzung erfolgt die Generierung in der Banking-App oder in einer eigenen TAN-App, zum Beispiel als Push-Nachricht.



… SMS auf Handy, Smartphone und Tablet

Der TAN-Empfang per SMS wird wahlweise als mTAN, mobile TAN oder auch SMS-TAN bezeichnet. Für das Verfahren benötigen Sie

eine aktive SIM-Karte. Nachdem Sie den Auftrag über Computer oder Tablet erteilt haben, wird Ihnen eine TAN per SMS auf Ihr Handy oder Smartphone gesendet. Den Zahlencode müssen Sie dann nur noch im Onlinebanking zur Freigabe des Vorgangs eingeben. Aus Sicherheitsgründen ist es ratsam, die SMS nicht auf dem Mobilgerät zu empfangen, das gleichzeitig für das Banking verwendet wird.

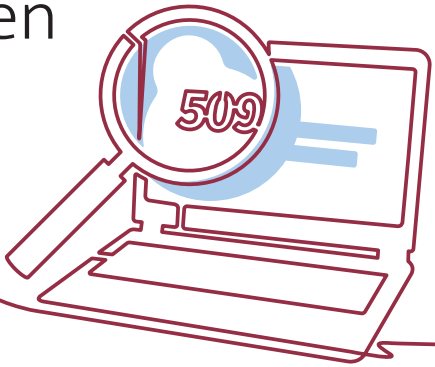


… Zusatzgerät per TAN-Generator

Auch hier werden zwei Geräte benötigt. Denn für die Erzeugung der TAN benötigen Sie eine spezielle Hardware, einen sogenannten TAN-Generator. Je nach Art des Geräts erfolgt die Generierung zum Beispiel mittels Chip der Bankkarte oder durch Scannen einer Grafik.

Übrigens: Die papierhafte iTAN-Liste kann weiterhin für bestimmte Aufträge genutzt werden. Daher bieten einige Banken die iTAN noch an.

Überweisungen **vornehmen**



Eine Überweisung führen Sie im Onlinebanking in einem zweistufigen Verfahren aus Eingabe und Freigabe aus. Zunächst tragen Sie – ähnlich einem Überweisungsbeleg – in einer Eingabemaske die Daten des Zahlungsempfängers ein. Kontrollieren Sie die Überweisungsdaten und leiten Sie dann den Auftrag an Ihre Bank. Diese fordert Sie nun zur Eingabe einer – nicht zweier oder mehrerer – TAN auf. Bevor Sie diese eingeben und die Zahlung somit freigeben, überprüfen Sie noch einmal die Überweisungsdaten – auch gegen den originalen Überweisungsauftrag oder Beleg.

Prüfen Sie nach Abschluss der Überweisung noch die Auftragsbestätigung. Einige Banken teilen Ihnen zudem eine Bestätigungsnummer für Rückfragen mit. Sehen Sie sich den aktuellen Kontostand und die zuletzt vorgenommene Überweisung in der Umsatzübersicht an: Stimmen Empfänger, Betrag, Verwendungszweck, Empfänger-IBAN? Sollte Ihnen eine Unstimmigkeit

auffallen, melden Sie diese bitte umgehend Ihrer Bank. Wird bei der Freigabe eine Fehlermeldung angezeigt, überprüfen Sie zunächst Ihre eingegebene TAN auf Tippfehler. Lässt sich der Fehler hierdurch nicht beheben, kontaktieren Sie Ihre Bank. Haben Sie bereits früher eine Überweisung an denselben Empfänger getätigt, ist die manuelle Eingabe häufig nicht notwendig. Banken bieten sogenannte Überweisungsvorlagen an, mit denen Sie Empfängerdaten für zukünftige Zahlungen abspeichern können. Auch wenn Sie eine Überweisungsvorlage nutzen, ist es immer sinnvoll, kurz zu prüfen, ob alle Daten richtig übernommen wurden. Denn ein Angreifer, der Zugriff auf Ihr Konto hatte, könnte versuchen, auch diese Vorlagen zu manipulieren, zum Beispiel indem er die IBAN für Ihre monatliche Mietzahlung ändert.

Beenden Sie die Onlinebanking-Sitzung korrekt, indem Sie auf „Logout“ oder „Abmelden“ klicken. Schließen Sie also nicht einfach den Internetbrowser oder die App. Zu guter Letzt: Kontrollieren Sie regelmäßig Ihren Kontoauszug bzw. online Ihre Konto-, Wertpapier- und Kreditkartenumsätze.

Tipps

Überweisungsdaten mit Beleg abgleichen

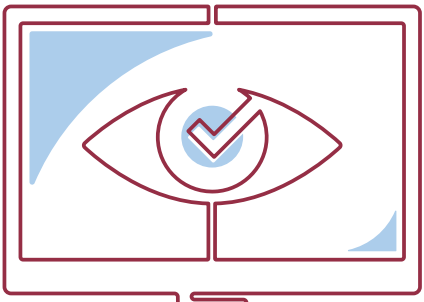
Nach Onlinebanking-Sitzung ausloggen

Kontostand regelmäßig überprüfen

Sicherheitseinstellungen **kontrollieren**

Prüfen Sie regelmäßig die Sicherheitseinstellungen Ihres Online- und Mobile-Bankings. So können Sie in der Regel Tageslimits für Überweisungen setzen oder ein festes Referenzkonto für Tagesgeldkonten hinterlegen. Durch das Limit können Sie festlegen, wie viel Geld maximal von Ihrem Konto einmalig oder in einem bestimmten Zeitraum überwiesen werden kann. Wenn Sie ein Referenzkonto eingerichtet haben, kann ein Dritter Ihr Geld online auf kein anderes Konto überweisen. Ferner sollten Sie regelmäßig auch Ihre bei der Bank gespeicherten persönlichen Daten wie Postanschrift, E-Mail-Adresse oder Handynummer prüfen und aktuell halten.

Wichtig: Viele Banken bieten ihren Kunden im Onlinebanking die Möglichkeit, den Zeitpunkt des letzten Online-Zugriffs einzusehen. Prüfen Sie daher den Zeitpunkt der letzten Anmeldung. Sollten Sie zu dem Zeitpunkt nicht angemeldet gewesen sein, hatte wahrscheinlich ein Fremder Zugriff auf Ihr Konto. Informieren Sie



in diesem Fall sofort Ihre Bank und ändern Sie Ihre Zugangsdaten. Merken Sie sich den Zeitpunkt Ihrer letzten Onlinebanking-Sitzung. Prüfen Sie Ihre Umsätze, Ihren Konto- und Depotstand. Sind alle Überweisungen, auch die vorgemerkten, von Ihnen veranlasst? Kontaktieren Sie anderenfalls umgehend Ihre Bank.

Tipps

Tageslimit festlegen

Persönliche Daten aktuell halten

Kontobewegungen prüfen

Mit Ihrer Erlaubnis: **Zugriff auf Ihr Konto**

Seit September 2019 sind Banken verpflichtet, sogenannten Drittdienstleistern einen Zugang zu Ihren Zahlungsverkehrskonten zu ermöglichen, wenn Sie als Kunde dies ausdrücklich wünschen. Dabei dürfen nur Dienstleister auf Ihre Konten zugreifen, die von der Bundesanstalt für Finanzdienstleistungsaufsicht überwacht werden. Drittdienstleister erhalten dadurch einen kontrollierten Zugriff auf Ihr Konto. Dies bedeutet, dass der Drittdienstleister über spezielle Schnittstellen die Infrastruktur Ihrer Bank nutzt, um bestimmte Informationen abzurufen. Hierbei lassen sich drei verschiedene Dienstleistungen unterscheiden, für die Sie online den Zugriff auf Ihr Konto ermöglichen können:

Kontoinformation: Sie können einen Drittdienstleister ermächtigen, Informationen zu Ihren Konten abzurufen, z. B. Umsätze oder Salden.
Zahlungsauslösung: Sie können ihn dazu berechtigen, eine Überweisung über Ihr Girokonto durchzuführen.
Deckungsprüfung: Mit Ihrer Genehmigung darf für ein Konto abgefragt werden, ob ein bestimmter Betrag verfügbar ist.

Um Ihnen die Kontrolle über die Zugriffe zu ermöglichen, bieten Ihnen viele Banken in der Nutzerverwaltung des Onlinebankings die Möglichkeit, die gewährten Kontozugriffe einzusehen, zu ändern oder zu entfernen.

Typische Gefahren: **Phishing und Schadsoftware**

Daten sind im digitalen Raum von großem Interesse – auch für Kriminelle. Dies betrifft ebenso Online- wie Mobile Banking. Zwei Varianten werden besonders häufig von Betrügern genutzt: Datendiebstahl per Phishing und die Verteilung von Schadsoftware.

Phishing – Abfischen von Daten

Der Begriff Phishing bezeichnet das Fälschen von Internetseiten, E-Mails oder Kurznachrichten wie SMS, um Daten auszuspähen. Bei Phishing-Angriffen versuchen Betrüger unter anderem, Sie per E-Mail oder auch über SMS auf die vermeintliche Onlinebanking-Website Ihrer Bank zu locken, um Ihre Daten abzufangen. Auf E-Mails oder SMS der vermeintlich eigenen Bank, die zu einer Bestätigung der sensiblen Daten auffordern, etwa über die Abfrage von PIN oder TAN, sollten Sie grundsätzlich nicht antworten. Öffnen Sie auch keine Links, die zu einer weiteren Eingabeseite führen. Ihre Bank fragt entsprechende Daten weder per E-Mail

Vorsicht, wenn Sie zu einer der folgenden Handlungen aufgefordert werden:

- Abfrage mehrerer TAN (Transaktionsnummern)
- TAN-Eingabe bei Androhung einer vermeintlichen Kontosperrung oder Laufzeitbeschränkung des TAN-Verfahrens
- Bestätigung Ihrer Kontodaten per TAN
- Rücküberweisung einer vermeintlich auf Ihrem Konto eingegangenen Zahlung
- Anmeldung zu einem Demo-Konto
- Durchführung einer Testüberweisung
- Installation von Sicherheitszertifikaten oder Sicherheitssoftware/-Apps

oder SMS noch telefonisch ab. Beenden Sie umgehend Telefonate, bei denen Sie ein vermeintlicher Bankmitarbeiter anruft und dazu drängt, gemeinsam eine Transaktion vom Konto durchzuführen.

Malware – Angriff per Schadsoftware

Als Malware werden schadhafte Programme auf dem PC oder mobilen Geräten bezeichnet. Schadsoftware kann beispielsweise

Ihre Tastatur- und Mauseingaben sowie Bildschirminhalte unbemerkt mitschneiden, manipulieren oder an Dritte weiterleiten.

Installiert werden diese häufig über das Öffnen unbekannter Dateianhänge oder das unbeabsichtigte Herunterladen von Software über manipulierte Internetseiten. Gängig sind vor allem Computerviren und Trojaner, die beispielsweise Transaktionsdaten verfälschen oder sensible Daten, wie Passwörter oder Kontaktdaten, ausspähen und weiterleiten.

Zur Verschleierung schaltet die Schadsoftware auch persönliche Sicherheitssoftware wie die Firewall oder das Antivirenprogramm aus. Unter Umständen kann ein Angreifer dann auf die infizierten Geräte zugreifen und die Kontrolle über alle Funktionen und Dateien erlangen. Damit übernimmt der Kriminelle Ihr Gerät, als säße er direkt davor oder hielte es in der Hand.

Stellen Sie sicher, dass Ihr Antivirenprogramm regelmäßig (mindestens wöchentlich) einen kompletten Suchlauf über alle Apps, Ordner und Dateien Ihres Gerätes durchführt. Sobald für Ihren PC, Ihr Smartphone oder Tablet eine Aktualisierung des Betriebssystems oder des Internetbrowsers verfügbar ist, sollten Sie diese umgehend installieren.

Arbeiten Sie am Computer nicht mit Administratorrechten oder mit Smartphones/Tablets, die gerootet[1] oder gejailbreakt wurden. Erlangt ein Angreifer Zugriff auf Ihr Gerät, kann er so alles damit machen. Insbesondere kann der Angreifer dann Sicherheitssoftware und Sicherheitseinstellungen Ihres Gerätes deaktivieren oder Schadsoftware installieren. Arbeiten Sie deshalb mit minimalen Nutzerrechten.

Gewähren Sie einer App nur die Berechtigungen, die sie zur Erfüllung ihrer Aufgabe zwingend benötigt. So benötigt zum Beispiel eine App zum Streamen von Musik keinen Zugriff auf Ihre Kontakte.

Infiziertes Gerät erkennen

Wie können Sie erkennen, ob Ihr Gerät infiziert ist? Achten Sie auf ungewöhnliches Verhalten bei der Nutzung Ihres Gerätes: Ignorieren Sie niemals Meldungen des Betriebssystems, Ihrer Sicherheits- und Anwendungssoftware sowie Ihrer Apps. Einfaches Wegklicken oder unbedachtes Zustimmen kann Schäden verursachen.

---

1 Nicht autorisiertes Entfernen von Nutzungsbeschränkungen. Bei Apple-Geräten spricht man von Jailbreaking, bei Android-Geräten von Rooting. Nach einem Jailbreak/Root kann das Gerät zum Beispiel Apps aus nicht autorisierten Quellen installieren.

Ist das Antivirenprogramm oder eine andere Sicherheitssoftware plötzlich nicht mehr aktiviert, so ist dies ein starkes Indiz dafür, dass Schadsoftware den jeweiligen Schutz manipuliert oder gar ausgeschaltet hat. Das Gleiche gilt auch für nicht funktionierende automatische Updates, zum Beispiel des Betriebssystems oder des Antivirenprogramms. Als Folge ist Ihr Gerät anfälliger und bei Angriffen weniger geschützt. Kontaktieren Sie in diesem Fall einen Fachmann und führen Sie keine Programme mehr auf Ihrem Gerät aus.

Informieren Sie sich regelmäßig über aktuelle Bedrohungen im Netz sowie über geeignete Schutzmaßnahmen. Informationen und Empfehlungen zu kostenfreier Sicherheitssoftware finden Sie auf der Website

- Ihrer Bank,
- der Polizei (www.polizei-beratung.de),
- des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi-fuer-buerger.de und www.botfrei.de) oder
- des Bankenverbandes (www.bankenverband.de).

Was tun bei **Verdacht?**

Haben Sie den Verdacht, dass Sie eine gefälschte Onlinebanking-Seite oder App Ihrer Bank genutzt haben oder dass ein Betrüger Zugriff auf Ihr Konto hatte, kontaktieren Sie umgehend Ihre Bank. Führen Sie auf keinen Fall Banking-Transaktionen aus, sondern besprechen Sie die weitere Vorgehensweise mit Ihrer Bank. Lassen Sie vorsorglich den Online-/Mobile-Banking-Zugang zu Ihrem Konto sperren.

Ist erkennbar, dass von Ihrem Konto bereits Geld abgeflossen ist oder andere unautorisierte Transaktionen vorgenommen wurden, informieren Sie umgehend Ihre Bank und erstatten Sie zudem Anzeige bei der Polizei. Zur weiteren Schadensabwehr sollten Sie auch Ihre Kreditkartenumsätze prüfen.

Überprüfen Sie in diesem Fall auch Ihren PC auf Schadsoftware und ziehen Sie hier gegebenenfalls einen Fachmann hinzu. Grundsätzlich gilt: Der beste Weg zu einem sauberen PC ist die Neuinstallation. Danach aktualisieren Sie Betriebssystem, Anwendungssoftware und Sicherheitssoftware (zum Beispiel Antivirenprogramm und Personal Firewall). Eine Aktualisierung ohne Neuinstallation ist gegebenenfalls nicht ausreichend. Erst jetzt sollten Sie auch die Zugangsdaten zu all Ihren Online-Diensten wie E-Mail-Konten, Onlineshops und sozialen Netzwerken ändern.

Onlinebanking – **nicht im Namen Fremder**

Auf Webseiten oder per E-Mail sprechen Kriminelle immer wieder Inhaber von Bankkonten an, um sie für eine Tätigkeit als sogenannter „Finanzagent“, „Warenagent“ oder auch „Kontovermieter“ zu gewinnen. Stellen Sie niemals Ihr Bankkonto Dritten – auch nicht Freunden – für Finanztransaktionen zur Verfügung. Über diese Betrugsarten informiert Sie ausführlich das Faltblatt „Dubioses Stellenangebot: Finanzagent“ des Bankenverbandes.

Wichtige Sicherheitstipps im Überblick

- Halten Sie Ihre Online- und Mobile-Banking-Geräte aktuell – das betrifft Software und Hardware.
- Aktivieren Sie automatische Updates auf all Ihren Geräten.
- Setzen Sie Sicherheitssoftware (Antivirenprogramm und Firewall) ein.
- Verwenden Sie immer die aktuelle Version Ihres Internetbrowsers/Ihrer Banking-App.
- Öffnen Sie keine E-Mails mit Anhängen und keine SMS von unbekannten Absendern.
- Beachten Sie die Sicherheitshinweise Ihrer Bank.
- Bleiben Sie aufmerksam.

So erreichen Sie den Bankenverband

Bundesverband deutscher Banken
Postfach 040307
10062 Berlin
+49 30 1663-0

bankenverband@bdb.de
bankenverband.de

Herausgeber:
Bundesverband deutscher Banken e. V.
Inhaltlich Verantwortlicher:
Oliver Santen
Gestaltung:
ressourcenmangel an der panke GmbH
Druck:
Buch- und Offsetdruckerei H. Heenemann GmbH & Co. KG

Berlin, April 2020