Digitale Panzerknacker

Banken PIN, TAN – und weg ist das Geld. Seit viele Bankgeschäfte online stattfinden, greifen Kriminelle bevorzugt im Internet an. Die digitalen Räuberbanden sind nicht nur eine Gefahr für Verbraucher, sie könnten auch eine neue Finanzkrise auslösen.

Sven David, 35 und Diplomingenieur bei einem großen Konzern, hielt seinen Firmenlaptop lange für eine uneinnehmbare Bastion. Die Festplatte: verschlüsselt, der Virenscanner: aktualisierte sich automatisch. „Die IT-Abteilung bei uns ist sehr gut“, sagt David. Deshalb hatte er keine Bedenken, auf dem Gerät, das er abends immer mit nach Hause nimmt, nach Feierabend auch seine Bankgeschäfte zu erledigen.

So auch im August 2014: David überwies für zwei kleine Einkäufe bei Ebay jeweils 20 Euro, am nächsten Tag fuhr er in den Urlaub. Als er zwei Wochen später zurückkam und seine Kontoauszüge checkte, stellte er fest: Es hatte kurz nach seinen Transaktionen noch eine dritte gegeben – allerdings nicht über 20, sondern über 1965 Euro. Der Empfänger: angeblich eine Gebäudetechnikfirma mit einem Konto in Valencia, Spanien.

David rätselt noch immer, wie das eigentlich passieren konnte. Seine Bank weigert sich bis heute, den Schaden zu bezahlen. Die Polizei weiß auch nichts Genaues, geht aber davon aus, dass möglicherweise seine Handy-SIM-Karte irgendwie kopiert wurde – David bekam damals die TANs für seine Überweisungen aufs Smartphone geschickt. Eine solche TAN müssen die Täter bekommen haben, obwohl David auch sein Handy schützte, so gut es ging.

Die Tricks der Onlinebankräuber werden immer perfider. Die Raubzüge im Internet sind ein Milliardengeschäft geworden, mit noch goldeneren Zukunftsaussichten. Schon jetzt erledigen allein in Deutschland etwa 38 Millionen Menschen ihre Überweisungen online, viele kaufen über das Netz Aktien und verwalten dort ihre Depots. Allein der Zahlungsdienstleister PayPal hat hierzulande 16 Millionen aktive Nutzer. Die digitalen Bankgeschäfte sind schnell, bequem und kostengünstig – aber sind sie auch sicher?

So offen wie Ingenieur David reden Betroffene selten über ihre Verluste, die Banken spielen das Problem herunter. Auch die offiziellen Zahlen sind wenig alarmierend: Laut Bundeskriminalamt lag der Gesamtschaden, den Internetkriminelle 2015 verursacht haben, bei lediglich 40 Millionen Euro. Doch das sind nur die angezeigten Taten, ein Bruchteil dessen, was tatsächlich geschieht.

Die Dunkelziffer, bei der Banken den Schaden stillschweigend ausgleichen oder erpresste Unternehmer und Bankkunden einfach zahlen, liegt wesentlich höher, sagen Kriminalisten und IT-Experten.

Der SPIEGEL hat mit zahlreichen Opfern von Onlineraubzügen gesprochen, mit Bankern, Hackern und Ermittlern. Der Befund ist so eindeutig wie alarmierend: Die schönen neuen Onlinebezahlwelten bergen immense Risiken – nicht nur für einzelne Kontoinhaber wie Sven David. Sondern für Banken, Börsen und das Finanzsystem insgesamt.

Wie ernst das Problem tatsächlich ist, zeigte sich vergangenen November: Da ließen deutsche Ermittler das international operierende Gangsternetzwerk

Avalanche hochgehen, das auf Hackingangriffe spezialisiert war. Allein der Schaden, den diese Diebesbande angerichtet hat, die nur eine von vielen ist, soll bei mehreren Hundert Millionen Euro weltweit liegen.

Vom einzelnen Geldautomaten bis zum internationalen Bankendienstleister Swift: Alle Glieder in der international total vernetzten Finanzwelt sind angreifbar – und sie werden angegriffen. „Die nächste Weltfinanzkrise könnte von einem Hackerangriff auf Banken ausgelöst werden“, sagt Mark Boleat, Berater und Finanzexperte in der City of London, einem der führenden Finanzplätze weltweit.

Verden an der Aller in Niedersachsen, kurz vor Weihnachten: Das 27 000-Einwohner-Städtchen mit dem hübschen historischen Stadtkern ist vor allem für seine Reitturniere berühmt. Dass von hier aus eine der größten Operationen im Kampf gegen die internationale Cyberkriminalität gesteuert wurde, wusste bis vor Kurzem kaum ein Bürger.

Vier Jahre lang hatte die Verdener Staatsanwaltschaft unter Leitung des Juristen Frank Lange eine internationale Ermittlertruppe zusammengestellt und angeführt, mit Kriminalisten, Sicherheitsexperten und Geheimdienstlern aus 39 Ländern. Das FBI, das US-Department of Justice, die europäische Polizeibehörde Europol – alle waren sie dabei.

Frank Lange, blaues Sakko, Brille, ist ein unauffälliger Typ, der in einer typischen Behörde arbeitet: Möbel und Böden sind grau und beigefarben, im Gang stehen Kisten mit alten Akten.

Doch der verstaubte Eindruck täuscht. Lange und seine internationale Truppe arbeiteten in einem „virtuellen Großraumbüro“, wie er das nennt: In verschlüsselten Foren konnten Kollegen etwa aus Deutschland, Japan oder den USA sekundenschnell Informationen austauschen.

Lange und seine Leute waren es, die das Netzwerk Avalanche hochgehen ließen, eine gigantische Infrastruktur, über die Hunderttausende Computer weltweit gekapert und ausgeraubt worden waren.

Die Täter waren in 180 Ländern aktiv. Allein bei der Staatsanwaltschaft Verden liefen 27 000 Anzeigen aus dem ganzen Bundesgebiet auf, die Avalanche zugeordnet werden, sagt der Staatsanwalt. Und das seien längst nicht alle Opfer, ist er sicher: „Damit haben wir keine zehn Prozent.“

Am Beispiel des enttarnten Netzwerks können die Ermittler nun nachvollziehen, wie ausgefuchst die Internetgangster mittlerweile vorgehen.

So linkten die Gauner Tausende Bankkunden, indem sie ihnen vermeintliche Fehltransfers vorgaukelten. Ein Lkw-Fahrer etwa berichtet, wie er auf eine Mail hereinfiel, die besagte, das Zollamt habe ihm fälschlicherweise 1880 Euro überwiesen. Brav drückte er den Button „Rücküberweisung“ – schließlich war sogar ein täuschend echter Auszug seines Kontos an-

gehängt, auf dem die 1880 Euro in den Buchungen auftauchten.

Viele Kunden fielen auf diesen Trick mit der vermeintlichen Falschüberweisung von Zoll- oder Steuerbehörden herein, sagt Jurist Lange. Oft sahen sie sogar auf ihrer Onlinebankingseite die vermeintlichen Fehlbuchungen angezeigt, wenn sie sich einloggten: Der Kontostand war scheinbar entsprechend in die Höhe gegangen, die Seiten waren manipuliert.

Auch Erpresserattacken fuhren die Avalanche-Trickser: Sie hackten die Computer von Privatpersonen, blockierten die Festplatten, sodass die Opfer beim Hochfahren ihres PCs plötzlich nur noch einen Warnhinweis sahen, der angeblich vom Bundesamt für Sicherheit in der Informationstechnik stammte – oder von der Gema. Auf dem Computer seien illegale Musik- oder Bilddateien gefunden worden, hieß es da, für die Wiederfreigabe des PCs müsse ein Bußgeld bezahlt werden.

Die Fülle der Angriffsmöglichkeiten, die die Avalanche-Infrastruktur bot, sei erschreckend gewesen, sagen die Ermittler. Über das Netzwerk sei es auch möglich gewesen, Webshops so lange mit Anfragen zu bombardieren, bis deren Website streikte. Passwörter und Zugangsdaten für Zahlungsdienstleister, Ebay- oder Amazon-Konten hätten wie am Fließband abgefischt und im Internet verscherbelt werden können. In welchem Maße das auch tatsächlich geschah, wissen die Ermittler noch nicht.

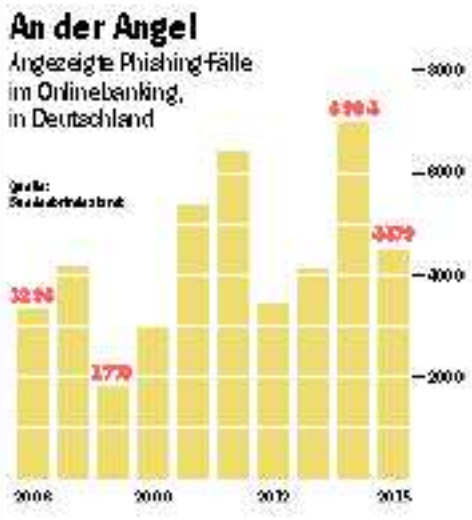
Damit das alles überhaupt möglich wurde, mussten die Täter Hunderttausende PCs weltweit über Trojaner kapern. Über diese Schadsoftware können Außenstehende Computer ausspionieren und kontrollieren. Früher kamen die Schädlinge meist als Anhang schlecht formulierter E-Mails daher, die mit gesundem Menschenverstand leicht als Fälschung auszumachen waren.

Doch auch hier hat sich die Branche professionalisiert. Täuschend echte Anschreiben, die vermeintlich von Amazon, PayPal oder Ebay kommen, bitten um eine Aktualisierung der Kundendaten oder mahnen eine vermeintliche Rechnung an. Die Details soll der Kunde angeblich im Anhang finden, hinter dem sich aber in Wahrheit eine Schadsoftware verbirgt. „Die Trefferquote dürfte vor allem vor Festen hoch sein“, sagt Andreas Klingbeil, Leiter eines Kommissariats Cybercrime beim Landeskriminalamt Berlin. „Wer hat beispielsweise vor Weihnachten nichts bei Amazon und Ebay bestellt?“

Auch PC-Nutzer, die Anhänge aus Prinzip nicht herunterladen und Links nie anklicken, sind nicht mehr geschützt. Schon ein gefälschter Facebook-Like-Button kann den Download starten. Oder die Schadprogramme lauern hinter vermeintlichen Werbeanzeigen, beispielsweise von Banken, die am Rande ganz normaler Websites stehen. Es reicht, wenn der Benutzer mit dem Mauscursor darüberfährt und kein Antivirenprogramm hat, das den Trojaner kennt. Schon hat er den Schädling auf dem Rechner.

Die gekaperten Computer werden von den Gangstern zunächst zu Tausenden zusammengeschlossen, zu sogenannten Botnetzen – Zombiearmeen, über die dann mit geballter Rechenkraft Attacken auf weitere Rechner gefahren werden. Allein die Telekom muss jedes Quartal rund 300 000 Kunden warnen, weil sie einen Trojaner auf ihrem Computer haben und Teil eines Botnetzes sind.

Smartphones wiederum werden von den Dieben über gefakte Apps gekapert, die per WhatsApp empfohlen werden und zwischenzeitlich auch schon mal im Google-Appstore zu finden sind. Oder die Hausbank bittet angeblich per SMS um eine Aktualisierung der Sicherheitseinstellungen. „Wenn das Smartphone dann kontrolliert wird, können die Täter Onlinebanking-TANs, die per SMS geschickt werden, abfangen und schlussendlich die Kontrolle über sämtliche Konten übernehmen“, sagt der Verdener Staatsanwalt Lange nüchtern. „Da werden dann erst einmal alle durchgeguckt, alles wird auf ein Standard-Girokonto überwiesen und das dann leer geräumt.“



Oft können sich die Betroffenen beim besten Willen nicht erinnern, wo sie sich die Malware eingefangen haben sollen. So wie Simon Radtke (Name geändert).

Er arbeitet als Geschäftsführer in einem Familienunternehmen in Norddeutschland und wurde innerhalb von drei Monaten gleich zweimal angegriffen. Erst verschwanden von seinem privaten Girokonto in zwölf Überweisungen fast 6000 Euro. Wenig später wurde das Familienunternehmen beinahe um 1,8 Millionen Euro erleichtert. Irgendjemand hatte im Namen Radtkes per E-Mail eine Mitarbeiterin angewiesen, für eine Firmenübernahme diese Summe an einen Herrn Baumann zu überweisen. Das Ganze war so perfekt inszeniert, dass sie keinen Verdacht schöpfte.

„CEO-Masche“ heißt der Trick, der vor allem in Frankreich und Österreich in Mode ist „und gerade massiv zu uns herüberschwappt“, wie der Berliner Kriminalhauptkommissar Klingbeil feststellt. Schließlich ist bei Unternehmen häufig mehr zu holen als bei Privatleuten, und gerade Kleinunternehmen haben oft kein Geld für ausgefeilte IT-Abwehrsysteme.

Die Täter betreiben einen erheblichen Aufwand. Radtkes Mitarbeiterin etwa bekam täuschend echte Mails, mit Anhängen, die zum Teil von der Finanzaufsicht BaFin zu kommen schienen. Auch der vermeintliche Herr Baumann meldete sich per Telefon.

Radtke bekam von der Millionenüberweisung nur per Zufall etwas mit: Er rief die Buchhalterin wegen einer anderen Angelegenheit an, da kam sie auf die Überweisung zu sprechen. „So konnte das Schlimmste noch verhindert werden.“ Mittlerweile hat die Firma die IT aufgerüstet und die Mitarbeiter entsprechend geschult. Trotzdem will Radtke seinen richtigen Namen nicht in der Zeitung nennen, aus Angst vor weiteren Angriffen.

Die knapp 6000 Euro, die von Radtkes Girokonto geklaut wurden, ersetzte ihm sein Geldinstitut – aber erst, nachdem er einen Anwalt eingeschaltet hatte. Denn längst gleichen Banken ihren Kunden Schäden durch Hackingattacken nicht mehr so kulant aus wie noch vor ein paar Jahren.

Der Rechtsanwalt Björn Vogel etwa verlor 31 000 Euro bei einem Hackingangriff. Als er im Frühjahr 2016 eine Kapitallebensversicherung ausgezahlt bekam, wurde das Geld ohne sein Wissen in 75 Tranchen an verschiedene ausländische Konten weiterüberwiesen.

Später stellte Vogel fest, dass jemand schon ein Jahr zuvor in seinen Bankingeinstellungen eine zweite Mobilfunknummer für die Überweisung der TANs hinterlegt hatte – und dann in aller Seelenruhe wartete, bis sich der Angriff lohnte.

Seit fast einem Jahr streitet sich der Jurist nun mit seiner Bank, wer den Schaden zu tragen hat. Erst bot das Institut 10 000 Euro „als reine Kulanzzahlung“ an, mittlerweile hat sie auf 18 000 Euro erhöht. So läuft es immer öfter.

Video: Die Masche der digitalen Bankräuber
spiegel.de/sp092017digital
oder in der App DER SPIEGEL

„Nur die Hälfte der Verfahren, die bei uns auflaufen, geht bei den Banken glatt durch und wird entschädigt“, sagt der Fachanwalt für IT-Recht Thomas Feil. Viele Häuser bauten offenbar darauf, dass die Anleger das finanzielle Risiko eines Gerichtsprozesses scheuten.

Theoretisch müssen Banken zwar bei einem „nicht autorisierten Zahlungsvorgang“ einspringen und dem Kontoinhaber den Betrag erstatten. Allerdings gilt diese Pflicht im Falle grober Fahrlässigkeit nicht.

Die aber ist schwer zu definieren. Außerdem dürften vielen Kunden eine oder mehrere Nachlässigkeiten nachzuweisen sein. Denn wer sich an alle Vorgaben der Banken hält, wie der PC oder das Smartphone zu schützen sind, hat ganz schön Arbeit. Virenscanner und Firewall sind stets aktuell zu halten, sämtliche Browser, Office-Anwendungen oder Handy-Apps ebenso. „Merken oder notieren Sie sich immer den Zeitpunkt Ihrer letzten Onlinebanking-Sitzung“, schreibt der Bankenverband gar in einem Ratgeber. „Ferner sollten Sie regelmäßig auch Ihre bei der Bank gespeicherten persönlichen Daten wie Postanschrift, E-Mail-Adresse oder Handynummer prüfen.“

Mit der gelebten Realität hat das wenig zu tun, sagt Kriminalhauptkommissar Klingbeil. „Was meinen Sie, wie viele Menschen hierherkommen und nicht einmal einen Virenscanner auf dem Laptop haben?“

Den Haag am 30. November 2016, kurz vor 14 Uhr: In einem schmucklosen Konferenzraum der Polizeibehörde Europol haben der Verdener Staatsanwalt Lange und an die dreißig weitere Beteiligte der Operation Avalanche den zentralen Kommandoposten bezogen.

Einige telefonieren per Handy, die meisten aber starren gespannt auf einen aufgehängten Bildschirm, über den ein Chat zu sehen ist, wie bei WhatsApp.

„Auf Position“, schreiben dort Kollegen aus aller Welt um kurz vor 14 Uhr. Einige Momente später stürmen im moldawischen Chişinău, im ukrainischen Poltawa, in Pittsburgh und in der Nähe von Berlin teils schwer bewaffnete Polizisten Wohnungen und Büros. In Poltawa kommt es zu einem Feuergefecht: Ein Mann ballert mit einer Kalaschnikow durch eine geschlossene Tür, verschanzt sich dann auf einem Balkon, kann aber wenig später festgenommen werden.

Parallel zu diesen Razzien arbeiten Softwarespezialisten fieberhaft an ihren Rechnern, sie müssen binnen kürzester Zeit 250 Server und 800 000 Domains beschlagnahmen oder blockieren, um so den Tätern den Zugriff auf Hunderttausende gehijackter Computer abzuschneiden. Diese könnten sonst innerhalb kurzer Zeit zu einem neuen Botnetz zusammengeschlossen werden.

Um Punkt 20 Uhr ist alles vorbei. Der polizeiliche Einsatzleiter meldet über den Chat an Lange und die internationalen Kollegen: „Avalanche is down!“ und: „Wonderful Work!“

Die wohl größte bekannte Botnetz-Infrastruktur weltweit ist nicht nur ausgeschaltet worden, es wurden auch fünf vermeintliche Strippenzieher festgenommen. Mehr als ein Dutzend weitere sind identifiziert, mehrere Haftbefehle ausgestellt. Das ist ein sensationelles Ergebnis für die Operation, findet Lange. An die Führungsspitzen der Cyberbanden kommen Ermittler nämlich nur selten heran.

Meistens enden die Untersuchungen bei den sogenannten Finanzagenten, den Geldwäschern der Onlinediebe. Die können über ihre Auftraggeber wenig sagen, oft wissen sie nicht einmal, dass sie mit

Gangstern zusammenarbeiten. Manchmal sind es einfache Senioren oder Hausfrauen, die nur eine kleine Nebentätigkeit ausüben wollten.

Geworben werden sie über harmlos klingende Annoncen. Das Avalanche-Netzwerk etwa suchte unter gefälschtem Firmennamen eine Zeit lang über Onlinejobbörsen wie Monster seine Helfershelfer, vermeintlich sollten sie für ein Unternehmen Bücher digitalisieren.

Sogar Bewerbungsgespräche per Telefon hätten stattgefunden, und dicke Arbeitsverträge seien verschickt worden, mit genauer Jobbeschreibung und Urlaubsregelung, sagt Lange. „Das Ganze wirkte sehr überzeugend."

Als Nächstes wurden die neuen Mitarbeiter angewiesen, sich für ihre Tätigkeit einen Hochleistungsscanner in einem bestimmten Internetshop auszusuchen, der der Fake-Firma angeblich Prozente gab. Das Geld für den Kauf bekamen sie scheinbar von ihrem Auftraggeber überwiesen, tatsächlich kam es vom Konto eines Hackingopfers und ging an ein unbekanntes Konto im Ausland, denn den Scannershop gab es natürlich auch nicht.

Meist werden die Finanzagenten nach einem oder wenigen Einsätzen ausgewechselt, sie sind zu leicht auffindbar für die Polizei. Von ihren Hintermännern haben sie dann oft nicht mehr als eine nicht mehr funktionierende Telefonnummer.

Über sie weiß man nur, dass sie häufig aus Osteuropa kommen. Die während der Avalanche-Ermittlungen festgenommenen Strippenzieher stammten aus der Ukraine und Aserbaidschan. Sicher ist außerdem, dass sie nicht nur erhebliche kriminelle Energie mitbringen, sondern auch beachtliche Programmierkenntnisse – und Organisationstalent. Sonst könnten sie eine Struktur wie Avalanche nicht managen. Das Netzwerk hatte allein in Deutschland mithilfe von eingeschleusten Trojanern zeitgleich 50 000 Computer von unwissenden Nutzern gekapert und diese zu verschiedenen Botnetzen zusammengeschlossen, über die dann gigantische Attacken gefahren wurden. Alle drei Monate wurden die Rechner im Schnitt ausgewechselt, die verwendeten Trojaner teils mehrmals täglich umprogrammiert, um die Virenscanner der Opfer wieder und wieder zu umgehen.

Obendrein nutzten die Gangster ihre Systeme nicht nur selbst, sondern vermieteten sie auch an Fremde. „Crime as a Service" heißt der gefährliche Trend bei Experten, der auch Kriminellen ohne tiefere IT-Kenntnisse den Einstieg in die Welt der digitalen Raubzüge erlaubt.

In den dunkelsten Ecken des Internets, im sogenannten Darknet, tummeln sich bereits jetzt unzählige Dienstleister, die alles Mögliche verscherbeln. Ihre Websites sind über einen speziellen Browser namens Tor erreichbar und meist nur auf Einladung zu betreten. Für manche wird neuerdings sogar eine Art Eintrittsgeld verlangt, zahlbar meist in der anonymen Kryptowährung Bitcoin.

Wer sich darauf einlässt, findet alles, was man braucht, um arglose Kreditkartenbesitzer, Bankkunden oder PayPal-Nutzer zu bestehlen. Die Shops sehen kaum anders aus als die von Amazon und Co., manche haben sich sogar das Fünf-Sterne-Bewertungssystem abgeschaut – für verlässlich gute, „heiße" und illegale Ware. Einige nutzen Webvideos, um sich selbst und ihre „Produkte" anzupreisen.

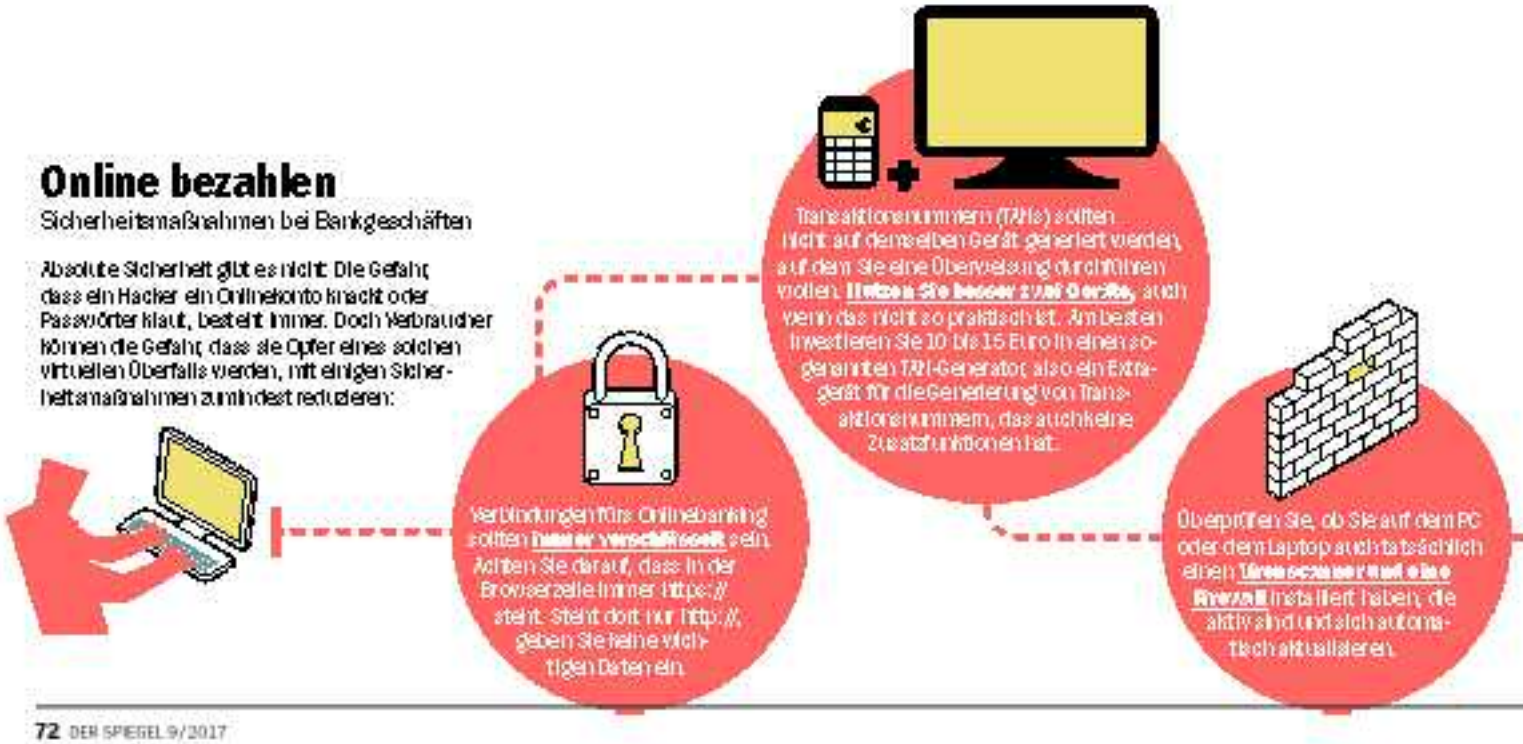
Angeboten werden beispielsweise Datenpakete zu einzelnen Kreditkarten, mit Namen, Adressen sowie dem dreistelligen Sicherheitscode auf der Rückseite, den man bei vielen Onlineeinkäufen per Kreditkarte angeben muss. 40 Euro kostet etwa ein solches Komplettpaket mit Daten europäischer Opfer aktuell.

Frankfurt am Main im Januar, im Handelssaal der Deutschen Börse: Die runden Waben, in denen Broker konzentriert auf Dutzende Bildschirme starren, dienen hauptsächlich als bunte Kulisse für die Börsennachrichten im Fernsehen. Tatsächlich läuft das Geschäft mittlerweile fast komplett virtuell, und wo so viel Geld bewegt wird, sind auch Kriminelle, die es darauf abgesehen haben, nicht weit.

„Als Börse sind wir ständig unter Beschuss, Angriffsversuche gibt es jede Woche", sagt Frank Fischer, Chief Security Officer des Hauses. Die gefährlichsten Angreifer suchen Schwachstellen in der IT, über die sie letztlich die Kontrolle über die Handelssysteme gewinnen könnten.

Haben sie Erfolg, könnten sie versuchen, den Handelsverlauf zu beeinflussen und mit eigenen Wetten Kapital daraus zu schlagen.

13 Millionen Mails gehen wöchentlich bei der Deutschen Börse ein, bis auf



400 000 werden alle ausgefiltert, und das ist nur die erste Verteidigungslinie. Der Handel wird permanent überwacht. Werden Angriffe entdeckt, reagiert eine schnelle Eingreiftruppe, das Cyber Emergency Response Team.

Die Vorkehrungen sind nicht übertrieben, denn mit der zunehmenden Professionalisierung der Cyberkriminalität geraten auch Börsen, Banken und Notenbanken stärker ins Visier der Täter – schließlich liegt hier sehr viel Geld.

Im Oktober 2010 initiierten Hacker einen Angriff auf die amerikanische Technologiebörse Nasdaq. Dort werden die Aktien von 3700 Unternehmen aus sechs Kontinenten im Wert von rund zehn Billionen Dollar gehandelt. Bräche dieses System zusammen, wären die globalen Folgen kaum abschätzbar. Die Angreifer schleusten in die Datenbanken Schadsoftware ein, die das Zeug hatte, die Nasdaq komplett zu zerstören – wäre sie nicht rechtzeitig entdeckt worden.

Nicht ganz so glimpflich verlief im Februar vergangenen Jahres ein weiterer Angriff auf die Infrastruktur des globalen Finanzsystems. Einer Gruppe von Hackern gelang es, Zahlungsaufträge über fast eine Milliarde Dollar im Namen der Notenbank von Bangladesch an die US-Notenbank Fed zu senden, betreffend das Dollarkonto der Bangladescher in New York.

Dass am Ende der Schaden bei nur 81 Millionen Dollar lag, war den mangelnden Orthografiekenntnissen der Gangster zu verdanken: Eine Zahlungsanweisung etwa forderte die New Yorker auf, 20 Millionen Dollar über eine Bank an eine Stiftung auf Sri Lanka zu überweisen. Doch wer auch immer den Auftrag initiiert hatte, schrieb das englische Wort für Stiftung falsch, aus „Foundation“ wurde „Fandation“.

Der Fehler fiel einem Mitarbeiter der Deutschen Bank auf, der die Überweisung abwickeln sollte. Eine Rückfrage bei der Notenbank von Bangladesch förderte die bis dahin vielleicht bedrohlichste Attacke auf das globale Finanzsystem zutage.

Den Hackern war über die Notenbank Bangladesch der Zugang zum zentralen Nervensystem des internationalen Finanzhandels gelungen: dem Telekommunikationsnetzwerk Swift.

Weltweit sind fast 11 000 Banken, Börsen und Broker an Swift angeschlossen. Sie senden über das System verschlüsselte Nachrichten hin und her, vorwiegend um Zahlungen rund um die Erde anzuweisen. Alle Swift-Nutzer verwenden Codes, über die sie sich identifizieren sowie einzelne Transaktionen kennzeichnen. Sie sind sozusagen die digitalen Schlüssel zu den Tresoren der Institute.

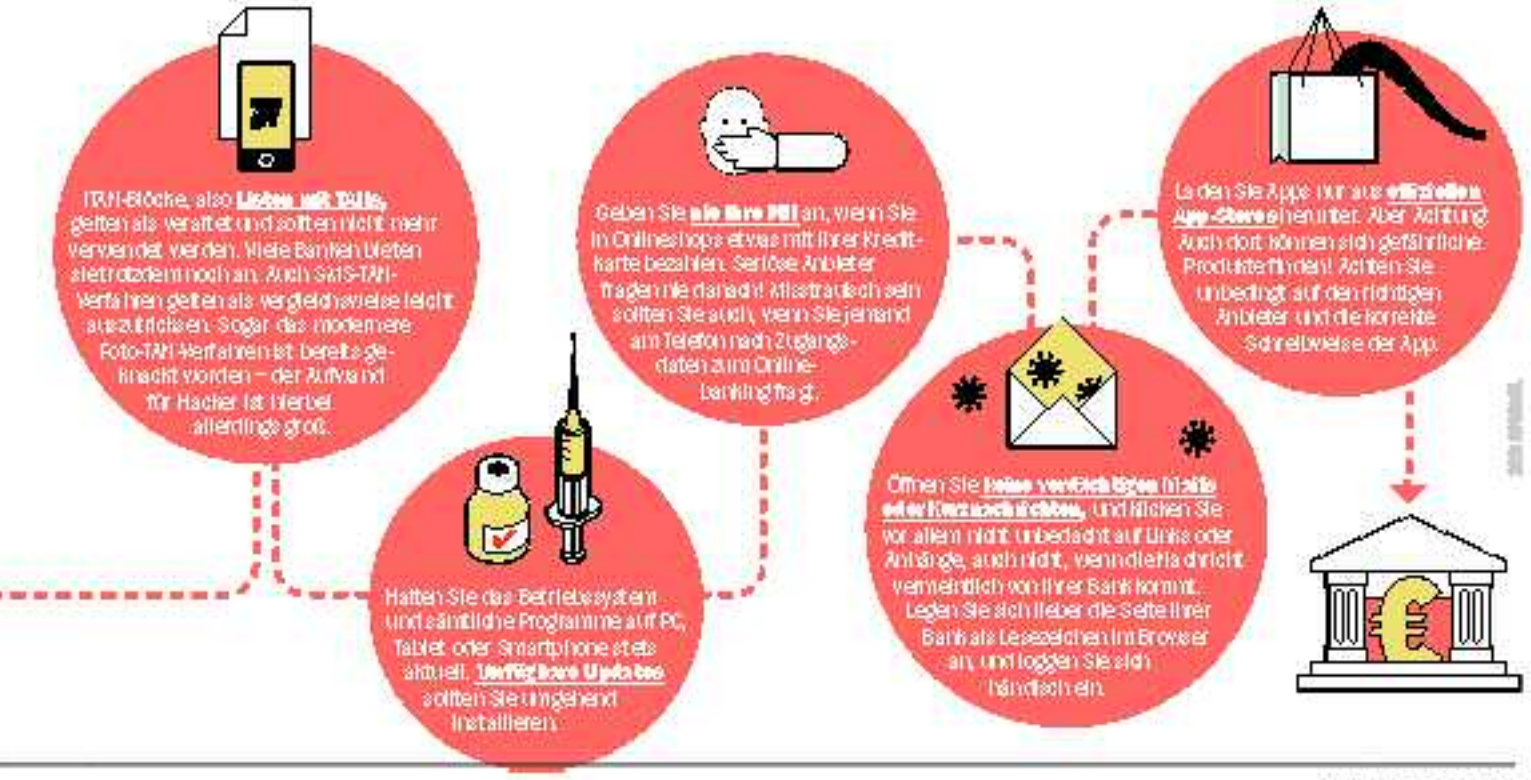
Die Bangladesch-Hacker gelangten an solche Codes. Swift-Chef Gottfried Leibbrandt betonte hinterher, der Fehler habe bei der Notenbank selbst gelegen und nicht bei Swift. Aber er warnte auch, es werde weitere Attacken dieser Art geben.

Schon jetzt hat sich seine Warnung bewahrheitet. „Es hat seit Bangladesch eine erhebliche Zahl weiterer Attacken gegeben, die einem ähnlichen Muster folgten – nicht nur in Asien, sondern auch in Europa und den USA“, sagt Anat Bar-Gera, Vorsitzende des Sicherheits-Joint-Venture Prosecs-Cyverse. In einigen Fällen sei es zu substanziellen Verlusten gekommen.

Wenn eine Bank zusammenbricht, kann das eine Kettenreaktion auslösen, das haben die Lehman-Pleite und die Finanzkrise von 2008 gelehrt. Jens Obermöller, Leiter des Referats für IT-Sicherheit bei der deutschen Finanzaufsichtsbehörde BaFin, sieht enorme Gefahren für das Bankensystem. „Cyberrisiken können durch die Vernetzung von Banken und der gesamten Finanzinfrastruktur zur Bedrohung für die Finanzstabilität werden“, sagt er.

Wie wahrscheinlich ein solcher Finanz-GAU ist, kann kaum jemand seriös voraussagen. Die BaFin selbst spielt Krisenszenarien durch, in denen nach einer Cyberattacke die IT-Infrastrukturen einzelner Banken oder Bankengruppen nicht mehr zur Verfügung stehen und beispielsweise Bargeldauszahlungen nicht mehr möglich sind. Ihr Hauptproblem ist, dass sich überhaupt nicht vorhersagen lässt, aus welcher Richtung die nächsten Angriffe kommen. Die IT-Infrastruktur der Geldinstitute ist oft hoffnungslos veraltet.

„Nach der Finanzkrise hat sich gezeigt, dass viele Banken lange Zeit zu wenig in ihre IT investiert und über viele Jahrzehnte ein System an das andere geflickt haben“, sagt François-Louis Michaud, Vizegeneraldirektor in der Bankenaufsicht der Europäischen Zentralbank (EZB). Zu lange waren die Banken vor allem auf Expansion getrimmt. Und es wuchs mit jeder Übernahme das Dickicht der Systeme.



Kaum einer dachte daran, dass sich daraus enorme Sicherheitslücken ergeben.

Mittlerweile stecken Banken zwar mehr in die Modernisierung und Sicherheit ihrer IT. Doch gleichzeitig sind im umkämpften Bankingmarkt neue Konkurrenten aufgetaucht: die sogenannten FinTechs, Start-ups, die rund um das Thema Finanzdienstleistungen neue Produkte entwickeln.

Und wieder steht Sicherheit oft nur an zweiter Stelle. Zwischen den Newcomern und den etablierten Banken ist ein Wettlauf ausgebrochen, wer am schnellsten die nächste schicke App an den Start bringt. Die Gefahr wächst, dass auch sicherheitstechnisch unausgereifte Techniken und Verfahren auf den Markt kommen.

Auch die BaFin ist bei dem Thema längst nicht so streng, wie sie sein müsste. Die IT-Infrastruktur wird bei der Lizenzvergabe der BaFin nicht tiefer gehend untersucht, der Gesetzgeber hat das schlicht nicht vorgesehen: Die Vorlage eines Organigramms, das entsprechende Sicherheitsvorkehrungen darlegt, reicht den geltenden Bestimmungen zufolge aus.

Die Ausarbeitung neuer Regeln und deren Umsetzung jedoch brauchen Zeit. Viel Zeit. Eine bereits beschlossene EU-Richtlinie etwa, die erstmals umfangreiche Anforderungen an den Einsatz des Smartphones beim Onlinebanking stellt, muss erst bis Anfang 2018 in nationales Recht umgesetzt werden.

Ein Jahr ist im Cyberkrieg eine Ewigkeit. Doch die Finanzwelt hat keine Zeit mehr.

„Der Angriff auf die Zentralbank von Bangladesch war ein Wendepunkt, der gezeigt hat, dass Cyberangriffe nicht mehr nur auf Bankkunden und ihre Guthaben abzielen, sondern nun auch die bankinternen Systeme ins Visier nehmen“, warnt Stephen Gilderdale, Chef des Kundensicherheitsprogramms von Swift.

Die für den globalen Zahlungsverkehr so zentrale Genossenschaft will nun den Druck auf ihre Mitgliedsbanken erhöhen, ihre Cyberabwehr zu stärken. „Die von Land zu Land unterschiedlichen Gesetze zur Cybersicherheit sind eine Herausforderung“, sagt Gilderdale. Auf neue, bessere Gesetze will man in der Swift-Zentrale bei Brüssel aber nicht warten.

„Wir wollen bis April einen neuen Sicherheitsstandard für Finanzdienstleister vorlegen“, kündigt Gilderdale an. „Das Ziel ist, alle Banken auf diesen Standard zu heben.“ Um das zu erreichen, will Swift ein Zertifizierungssystem etablieren: Banken berichten Swift in einer Art Selbstauskunft, wie sie die neuen Standards umsetzen – bis Ende dieses Jahres müssen sie liefern. Schon jetzt besitzt Swift eine Datenbank mit Informationen aus den Know-Your-Customer-Programmen der Banken, mit denen die Nutzer des Kommunikationsnetzes präventiv gegen Geldwäsche vorgehen. Mittelfristig wird diese Datenbank erweitert, sodass sie auch Informationen zu den attestierten Sicherheitsstandards der Kunden enthalten wird.

Gesetzlich verpflichtend sind die neuen Regeln nicht. Doch Swift erwartet, dass Banken selbst beginnen werden, nur noch mit Instituten Geschäfte zu machen, die ein positives Audit vorweisen können. Geht die Rechnung auf, könnten weniger sichere Banken in Zukunft Probleme bekommen, am internationalen Zahlungsverkehr teilzunehmen.

Ab 2018 sollten die Swift-Informationen über die attestierte Sicherheit der Banken auch den jeweils zuständigen Aufsichtsbehörden zur Verfügung gestellt werden, zum Beispiel der EZB.

Und auch die erhöht den Druck. Die EZB will ihr eigenes Arsenal zur Bekämpfung von Cyberrisiken erweitern, erwägt etwa, sogenannte ethische Hacker in die Banken zu schicken, die Schwachstellen im System aufspüren und testen, inwieweit Sicherheitslücken die Bank als Ganzes gefährden könnten.

Ob behäbige Institutionen wie eine Zentralbank im Wettlauf mit den Angreifern schnell genug sind? Die Cyberkriminalität entwickelt sich rasant, und die zunehmende Digitalisierung aller Lebensbereiche eröffnet ihr immer neue Möglichkeiten.

Deutschland mit seinem zersplitterten Bankenmarkt und den vielen kleinen und mittleren Instituten ist besonders anfällig für Angriffe. Schließlich dürfte die IT-Abwehr vieler kleiner Häuser schon aus Kostengründen mit denen großer Institute kaum mithalten können.

Erschreckend viele Banken setzen außerdem auf veraltete Onlinebanking-Verfahren. Bei der Deutschen Bank, der Comdirect oder der ING-DiBa etwa ist noch immer das überholte iTAN-System im Einsatz. Santander und die Targobank geben an, dass es sogar das meistgenutzte System sei.

Die Politik reagiert langsam, die Banken sind behäbig. Und die Kunden ahnen meist nicht einmal, welche Risiken sie sich mit jeder Überweisung, jeder eingegebenen PIN, jedem Aktienkauf über das Internet einhandeln. Die meisten Deutschen beschäftigen sich kaum mit dem Thema, sie hoffen, dass sich schon irgendwer für sie darum kümmert. Sie lassen sich einlullen von dem Einfach-und-sorglos-Marketing der Onlinebanking-Anbieter.

Bankkunden, die Onlinebanking betreiben wollen, bleibt aber nichts anderes übrig, als sich in Zukunft stärker um die Sicherheit des eigenen Geldes zu sorgen. So einfach, wie es Banken und App-Anbieter suggerieren, ist die digitale Bezahlwelt nicht. Leider.

Markus Böhm, Angela Gruber, Martin Hesse, Henning Jauernig, Marcel Rosenbach, Anne Seith

Mehr zum Thema ab Montag auf SPIEGEL ONLINE unter spiegel.de/netzwelt