Redaktionsgespräch mit Arne Schönbohm

„Man kann das Thema IT-Sicherheit nicht ad acta legen“

Herr Schönbohm, das Jahr 2020 fing mit einem prominenten Fall einer Cyberattacke auf eine deutsche Bank an. Dabei wurde bei der DKB eine doch recht veraltete Angriffsart mit einem Distributed Denial of Service (DDoS) genutzt. Die Internetbank war stundenlang nicht erreichbar. Sollten solche Angriffe nicht mittlerweile abwehrbar sein?

DDoS-Angriffe sind eine weit verbreitete Angriffsart, deren Durchschlagskraft in den vergangenen Jahren sehr deutlich zugenommen hat. Sie werden meist mithilfe von Botnetzen durchgeführt, die oft aus sogenannten IoT (Internet of things)-Geräten bestehen. Das sind zum Beispiel Kühlschränke, Babyfone oder Rollladensteuerungen aus einem Smart Home, die mit dem Internet verbunden und leider oft schlecht geschützt sind. Dennoch kann man sich etwa mithilfe spezialisierter Dienstleister dagegen schützen. Zur Orientierung bietet das BSI etwa eine Liste qualifizierter DDoS-Mitigation-Dienstleister an.*

Hier gibt es also zwei Herausforderungen: Zum einen müssen die Geräte so sicher gestaltet werden, dass sie nicht zum Angriffswerkzeug werden können. Das kann zum Beispiel jeder leicht durch individuelle Passwörter regeln, anstatt die Voreingestellten einfach zu belassen. Zum anderen sollten Unternehmen nicht nur gute Krisenreaktionspläne in der Schublade haben, sondern diese auch immer wieder üben. Gerade in der streng regulierten Finanzwirtschaft sollte dies gelebte Realität sein, um eben ständig die Verfügbarkeit der Dienstleistung zu gewährleisten.

„Unternehmen sollten Krisenreaktionspläne nicht nur haben, sondern sie auch immer wieder üben.“

Der Angriff beeinträchtigte eine Tochterfirma der Finanz Informatik, welche unter anderem Dienstleistungen für die DKB erbringt. Besteht die Gefahr, dass durch den Trend zum zentralen Outsourcing solch sensibler Bereiche ganze Sektoren des Bankwesens „ausgeschaltet“ werden können?

In der Tat haben wir in der jüngeren Vergangenheit vermehrt gezielte Cyberangriffe auf IT-Dienstleister beobachtet, unabhängig von der Branche. Sie sind für Cyberkriminelle ein interessantes Ziel, weil mit der Zahl der Opfer der Leidensdruck und damit die Motivation ein Lösegeld zu bezahlen natürlich deutlich ansteigt. Daneben kann es auch für das Gemeinwohl zu einem ernsten Problem werden, wenn nach einem Angriff auf einen zentralen Dienstleister statt einem gleich ein gutes Dutzend Krankenhäuser erhebliche IT-Ausfälle hat.

Einen solchen Fall hat es 2019 in Deutschland bekanntermaßen gegeben, wir reden hier also über sehr realistische Szenarien. Mit einer Zentralisierung von Dienstleistungen entsteht immer auch ein Single-Point-of-Failure. Das sollte bei einer solchen Entscheidung immer berücksichtigt und für entsprechende Redundanzen gesorgt werden.

Ist in letzter Zeit eine steigende Zahl von Cyberangriffen auf die deutschen Banken zu verzeichnen?

Es gibt immer wieder Cyberangriffe auf die Finanzwirtschaft. Meist werden diese erfolgreich abgewehrt und sind daher für die Kunden gar nicht wahrnehmbar. Ein Trend ist hier derzeit nicht erkennbar. Oftmals haben Ausfälle ganz andere, recht triviale technische Ursachen, die aber für Kunden die gleichen unangenehmen Folgen haben können. Auch derartige Risiken sollten im Sinne eines Informationssicherheitsmanagement-Systems beachtet werden.

Würden Sie die deutsche Kreditwirtschaft als ausreichend vorbereitet für die zunehmenden Cyberrisiken bezeichnen?

Ja, denn die Unternehmen haben ein hohes Eigeninteresse an einem störungsfreien Geschäftsbetrieb, der im Wesentlichen auf IT-Systeme angewiesen ist. Daneben handelt es sich um eine verhältnismäßige stark regulierte Branche, in der schon vor dem seit 2015 geltenden IT-Sicherheitsgesetz Regelungen galten. Dennoch muss das IT-Sicherheitslevel eines Unternehmens immer im Einzelfall bewertet und dann auch bei Zweifeln gezielt gegengesteuert werden.

Finanzdienstleister, die zu den kritischen Infrastrukturen zählen, müssen dazu IT-Sicherheitsmaßnahmen nach dem Stand der Technik nachweisen. Nicht bei allen fiel diese Prüfung zufriedenstellend aus.

Für uns ist ganz wichtig, dass IT-Sicherheit als Daueraufgabe verstanden wird. Man kann nicht zu einem Tag X bestimme IT-Schutzmaßnahmen umsetzen und dann das Thema ad acta legen. Dafür ist das Feld viel zu dynamisch.

Was muss bei den Banken besser werden, um das Problem im Griff zu haben?

Wir untersuchen das derzeit. Dafür werten wir die im 2. Halbjahr 2019 erstmalig fälligen Prüfungsnachweise der so regulierten Unternehmen aus. Erste Ergebnisse zeigen, dass in der Breite durchaus noch Handlungsbedarf besteht, um die gesetzlichen Anforderungen vollständig zu erfüllen.

Hat das BSI auch einen Hebel, um die Banken dazu zu bewegen, mehr Ressourcen in die Abwehr von Cyberangriffen zu investieren?

Das BSI als Cybersicherheitsbehörde des Bundes verfolgt in erster Linie einen kooperativen Ansatz, um gemeinsam mit Betreibern, Partnern und Experten die Informationssicherheit zu erhöhen. Darüber hinaus zählen die größeren Kreditinstitute in der Regel zu den Betreibern der kritischen Infrastruktur Deutschlands. Diese sind durch das BSI-Gesetz dazu verpflichtet, Vorsorge in allen Bereichen zu betreiben. Über die Erfüllung dieser Anforderungen müssen die regulierten Unternehmen dem BSI regelmäßig Nachweise vorlegen. Diese Form der Regulierung kam nun erstmals im 2. Halbjahr 2019 zum Tragen. Verstöße können übrigens mit Bußgeldern geahndet werden. Darüber hinaus kann das BSI, vergleichbar mit den Aufsichtsbehörden der Finanzaufsicht selbst Prüfungen bei diesen Betreibern durchführen.

Stehen Sie im Austausch mit den Aufsichtsbehörden der Banken?

Selbstverständlich arbeiten wir eng mit der BaFin zusammen. Auch mit der Bundesbank oder der Europäischen Zentralbank stehen wir in regelmäßigem Kontakt und tauschen uns intensiv aus.

Neben dem Bedarf, mehr finanzielle Mittel zu investieren, ist aber auch der Personalmangel ein großes Thema. Echte Fachkräfte in diesem Segment sind rar und heiß umkämpft. Das BSI hat ja jüngst den neuen Studiengang „Cyber-Security" erschaffen. Was können Banken selbst tun, um die Personalsituation in den entsprechenden Abteilungen zu verbessern?

Da geht es insbesondere auch um die entsprechende Wertschätzung. IT-Sicherheitsspezialisten müssen in ihren Häusern gehört und in die wichtigen Projekte einbezogen werden. IT-Sicherheit muss Chefsache sein und das bedeutet, dass die Chefs den Experten zuhören und die nötige Unterstützung geben.

Ende 2019 trat die Payment Services Directive 2 (PSD2) in Kraft. Banken müssen nun ihre Schnittstellen auch für andere Dienstleister öffnen. Ist das ein mögliches Einfallstor und hat das bereits zu einem messbaren Anstieg der Angriffe geführt?

Die PSD2 erfordert die Bereitstellung einer Schnittstelle von allen Banken. Dienstleister dürfen dann mit Zustimmung des Kontoinhabers Zahlungen auslösen und Kontobewegungen abfragen. Die konkrete Ausgestaltung der Schnittstelle ist bislang nicht vorgegeben. Die dem BSI vorliegenden Informationen zu Cyber-Sicherheitsvorfällen lassen keinen derartigen Anstieg erkennen.

Sind andere Wirtschaftszweige in Deutschland besser vorbereitet als die Finanzwirtschaft?

Angesichts der zahlreichen Abhängigkeiten in den Wertschöpfungsketten unserer Wirtschaft würde eine derartige Einzelbewertung kein zuverlässiges Bild ergeben. Allein mit Blick auf die Bankinstitute wird offensichtlich, dass eine zuverlässige Dienstleistungserbringung heute von einer Vielzahl externer Infrastrukturdienstleistungen sowie einem komplexen Zusammenspiel unterschiedlicher Akteure des Finanzsektors abhängig ist. Diese Abhängigkeiten zeigen, dass eine angemessene Absicherung der gesamten Wertschöpfungskette gewährleistet werden muss, um eine ausreichende Resilienz des Systems zu gewähr-

„Nicht bei allen Finanzdienstleistern fiel die Prüfung der IT-Sicherheitsmaßnahmen zufriedenstellend aus."

Arne Schönbohm

Präsident, Bundesamt für Sicherheit in der Informationstechnik, Bonn

Mittlerweile ist vonseiten des Bundeskriminalamtes bekannt, dass eine Cyberattacke auf die DKB Anfang 2020, die Kunden stundenlang den Zugriff auf ihre Konten verwehrte, wohl durch zwei gelangweilte Jugendliche verschuldet wurde. Arne Schönbohm diskutiert im Gespräch, wie nahezu jeder Sicherheitslücken ausnutzen und sie gegen Unternehmen verwenden kann. Für den Schutz vor solchen noch recht einfachen Angriffen empfiehlt er einige Maßnahmen, die ohne großen Aufwand umzusetzen sind. Jedoch weist er darauf hin, dass Cyberangriffe auch in anderem Maße und von wesentlich professioneller organisierten Tätern durchgeführt werden können. Somit sei Cybersicherheit für Kreditinstitute, welche zur kritischen Infrastruktur Deutschlands zählen, heute einer der wichtigsten Aspekte, der bei der Planung und Umsetzung von Digitalprojekten einbezogen werden muss und nicht auf die lange Bank geschoben werden sollte. (Red.)

leisten. Die Regulierung der kritischen Infrastrukturen in Deutschland trägt diesen Abhängigkeiten durch die Einbeziehung zum Beispiel der Stromversorgung, aber auch der Bargeldlogistik oder der Kartenzahlungsinfrastruktur Rechnung.

Angenommen, ein größerer konzertierter Angriff legt tatsächlich eine Gruppe von Banken lahm: Gibt es Notfallpläne des Bundes für solche Szenarien, um die Versorgung der Wirtschaft mit Liquidität aufrechtzuerhalten? Oder sind solche extremen Angriffsszenarien auszuschließen?

Ein solches Szenario ist grundsätzlich nicht auszuschließen, auch wenn es zunächst nicht sehr wahrscheinlich erscheint. Deshalb muss die Bundesrepublik auch auf scheinbar extreme Krisenszenarien vorbereit sein. Die Bundesressorts haben 2016 unter Koordinierung des BMI ein neues Gesamtkonzept der Bundesregierung für die zivile Verteidigung erarbeitet. Das berücksichtigt natürlich auch die Finanzwirtschaft.

Die DKB hat bei dem Angriff im Januar eine kriminelle Motivation vermutet. Im Zeitalter der zunehmenden geopolitischen Spannungen wird aber auch immer öfter vor staatlichen Angriffen gewarnt. Auch das Finanzwesen wird als kritische Infrastruktur gewertet, die Ziele solcher staatlichen Sabotageakte werden könnte. Was ist Ihrer Meinung nach die größere Bedrohung für die Banken, Kriminelle oder staatliche Sabotage?

Der bei weitem größte Anteil der Cyberangriffe hat eine finanzielle Motivation und kommt aus dem Umfeld der organisierten Kriminalität. Das schließt Angriffe mit dem Ziel der Sabotage natürlich nicht aus. Die Cyberangriffe unterscheiden sich dabei nicht wesentlich, lediglich das Ziel ist dann ein anderes. Allerdings ist das für das BSI zunächst einmal nachrangig. Unternehmen jeder Branche sollten sich und ihre IT-Infrastruktur so aufstellen, dass sie gegen jede Form von Cyberangriffen zuverlässig geschützt sind.

Sie haben im Mai 2019 auf dem Bundesbank-Symposium darauf hingewiesen, dass das Thema quantenresistente Verschlüsselung uns noch intensiv beschäftigen wird. Im Oktober 2019 hat Google den Durchbruch mit Quantencomputern verkündet. Dieser hat erstmals eine Aufgabe gelöst, an der herkömmliche Rechner scheitern würden. Muss das Thema jetzt schon in naher Zukunft verstärkt auf die Agenda oder dauert das noch lange, bis diese Technologie auch im Alltag und vor allem für Hacker nutzbar ist?

Die Frage, ob oder wann Quantencomputer Realität werden, stellt sich nicht mehr. Allein schon aus Gründen des Risikomanagements ist mittel- bis langfristig ein Umstieg auf Quantencomputer-resistente Verfahren zwingend. Denn die Sicherheit digitaler Infrastrukturen beruht wesentlich auf Verfahren zur Schlüsselvereinbarung sowie für digitale Signaturen, die sich auf die angenommene Schwierigkeit bestimmter mathematischer Probleme stützen. Mit heutigen Mitteln sind die gängigen Public-Key-Verfahren nicht zu brechen. Dies gilt jedoch nicht mehr, wenn universelle Quantencomputer mit ausreichender Leistungsfähigkeit verfügbar sind. Globale IT-Konzerne und Staaten investieren daher erhebliche Beträge in die Entwicklung von Quantentechnologien und haben damit bereits beachtliche Fortschritte erzielt.

Zwar schätzt das BSI kurzfristige Entwicklungssprünge als eher unwahrscheinlich ein. Für kryptografische Anwendungen, die Informationen mit langen Geheimhaltungsfristen und hohem Schutzbedarf verarbeiten, ergibt sich dennoch akuter Handlungsbedarf. Hier besteht eine Gefahr darin, dass Nachrichten zur Schlüsselaushandlung sowie die mit den ausgehandelten Schlüsseln verschlüsselten Daten auf Vorrat gesammelt und in der Zukunft mithilfe eines Quantencomputers entschlüsselt werden.

> „Der überwiegende Anteil der Angriffe kommt aus dem Umfeld der organisierten Kriminalität."

Derzeit befindet sich das IT-Sicherheitsgesetz 2.0 auf dem Weg durch die Gremien. Dort soll es drastische Änderungen geben. Verstöße sollen künftig mit bis zu 20 Millionen Euro anstatt 100 000 Euro geahndet werden können, nur als Beispiel. Wird es Änderungen an den Auflagen geben, die insbesondere für die Banken Auswirkungen haben?

Zu aktuellen Gesetzgebungsverfahren möchte ich mich nicht im Detail äußern.

Welchen Rat würden Sie angesichts all Ihrer Erfahrungen den Banken für 2020 mit auf den Weg geben?

Ohne Cybersicherheit wird die Digitalisierung insgesamt und insbesondere auch in der Finanzwirtschaft nicht erfolgreich verlaufen. Speziell bei neuen Produkten und Dienstleistungen sollte die IT-Sicherheit schon während der Entwicklung berücksichtigt werden. Kooperation und Verständigung sind hier das A und O. Das BSI bietet hierfür eine integrierte Wertschöpfungskette von Angeboten mit Fokus Cybersicherheit für die Wirtschaft und insbesondere für KRITIS-Betreiber an.

> „Bei neuen Produkten sollte die IT-Sicherheit schon während der Entwicklung berücksichtigt werden."

* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.html