Johannes Beermann / Arne Schönbohm

Hacken für die gute Sache – **Cybersicherheit** auf dem Prüfstand

Schwerwiegende IT-Sicherheitsvorfälle gab es in den vergangenen Jahren so häufig wie nie zuvor. Betroffen waren Krankenhäuser in Großbritannien, Energieversorger in der Ukraine, Autohersteller in Frankreich, Polizeibehörden in Indien oder auch die Deutsche Bahn – um nur wenige Beispiele aus einer sehr langen Liste zu nennen. Cyberkriminelle kennen keine Landesgrenzen und hinter den Angriffen stecken vielfältige Motive. Oft verfolgen Täter finanzielle Interessen, aber gerade die besonders medienwirksamen Angriffe waren häufig politisch motiviert oder sogar staatlich gelenkt.

Internationaler Zahlungsverkehr als Ziel von Attacken

Spätestens seit dem spektakulären Bankraub von Bangladesch im Jahre 2016 gelten Cyberrisiken auch im Finanzsektor als eine der größten Bedrohungen. Damals entwendeten Cyberkriminelle 81 Millionen US-Dollar. Sie initiierten Überweisungen an Banken im Ausland über das SWIFT-Netzwerk, nachdem sie vorher über eine längere Zeit unentdeckt die internen Prozesse der Zentralbank von Bangladesch ausspionieren konnten. Die entwendeten Gelder lagen dabei nicht einmal in Bangladesch selbst, sondern auf der anderen Seite der Welt auf einem Konto bei der Federal Reserve Bank in New York.

Insbesondere der internationale Zahlungsverkehr ist schon lange ein globales Geschäft mit oft komplexen, langen Prozessketten und vielen Akteuren. Jedes einzelne Glied in der Kette könnte ein potenzielles Einfallstor für Angreifer darstellen. Auch ein gut geschütztes Institut kann also durch einen Cyberangriff bei einem Dritten zu Schaden kommen und sei es nur durch die beschädigte Reputation.

Gemeinsames Vorgehen – national wie international

Der Schutz vor Cyberrisiken ist somit keine Sache des Einzelnen, sondern erfordert ein gemeinsames Vorgehen aller Marktteilnehmer – national wie international. Deshalb hat der Netzwerkbetreiber SWIFT als Reaktion auf den Vorfall in Bangladesch die Anforderung an die Teilnahme an seinem Netz verschärft. Mit dem sogenannten Customer Security Programme hat SWIFT seine Teilnehmer verpflichtet, ein gewisses Maß an IT-Sicherheit einzuhalten (zum Beispiel verpflichtende Sicherheitsupdates, Anforderungen an Passwörter, Anforderungen an den physischen Zugang zur Hardware) und eine Bewertung ihrer IT-Sicherheit durchzuführen.

Über das BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Als unabhängiges Kompetenzzentrum für IT-Sicherheit in Deutschland, als Multiplikator und zentrale koordinierende Stelle verfolgt das BSI die ganzheitliche und konsistente Implementierung seiner vielfältigen Aufgaben, beispielsweise im Bereich der Cyber-Sicherheitsstrategie.

Wissen aus der operativen Cyberabwehr sowie erzielt durch permanente Hard- und Softwareanalysen beziehungsweise im Bereich der Verschlüsselungstechnologien kann für Standardisierung und Zertifizierungen eingesetzt werden. Mit dieser Strategie gestaltet das BSI IT-Sicherheit aus einer verantwortlichen Position. Es agiert in einem kooperativen Ansatz mit zahlreichen Partnern und Experten zu unterschiedlichen Aspekten der IT-Sicherheit. Wissen und Informationen aus der Lagebeobachtung, zu Bedrohungen, Schwachstellen und Angriffen auf die Informationstechnik sowie resultierend aus der Auswertung von IT-Störungen, die im Nationalen IT-Lagezentrum als Meldungen eintreffen, kann unter anderem in der Erstellung und gezielten Weiterleitung von Cyber-Sicherheitswarnungen und Hilfsempfehlungen an vielfältige Adressatenkreise in Staat, Wirtschaft und Gesellschaft münden.

Ein prominentes Beispiel hierfür sind die jüngsten BSI-Warnmeldungen im Zusammenhang mit Cyberangriffen auf deutsche Energieversorger* und andere kritische Infrastrukturen, die ein deutliches Signal an die Unternehmen senden, ihre Computersysteme noch besser zu schützen.

* Vergleiche hierzu die entsprechende Pressemitteilung des BSI: https://www.bsi.bund.de/DE/Presse/

Jedes an SWIFT angebundene Institut kann sich die Umsetzung dieser Maßnahmen von seinen Geschäftspartnern bestätigen lassen und unter anderem auf dieser Basis entscheiden, ob die Geschäftsbeziehung aufgenommen, fortgesetzt oder beendet werden soll. In Deutschland hat mittlerweile die große Mehrzahl aller Banken eine solche Bestätigung abgegeben. Die SWIFT-Anforderungen an die IT-Sicherheit haben in vielen Häusern zu einer Aufrüstung der IT-Sicherheit geführt.

Die Deutsche Bundesbank begrüßt das Customer Security Programme von SWIFT und die damit einhergehende Steigerung der Cybersicherheit im Zahlungsverkehr. Dennoch sind weitere Bemühungen aller Beteiligten erforderlich, um auch den deutschen Finanzsektor nachhaltig vor Cyberangriffen zu schützen. Die deutschen und europäischen Behörden haben schon einige Maßnahmen initiiert.

Einsatz von „Red Teams"

Jüngstes Beispiel ist „TIBER-EU" (Threat Intelligence-based Ethical Red Teaming): Ein europäisches Rahmenwerk, welches von der Europäischen Zentralbank unter Mitwirkung von Bundesbank und anderen nationalen Notenbanken Europas entwickelt und im Mai dieses Jahres veröffentlicht wurde. Das Rahmenwerk ist in erster Linie auf Finanzmarktinfrastrukturen wie zum Beispiel Zahlungsverkehrssysteme anwendbar. Perspektivisch können die „Red Teams" aber auch über den Finanzsektor hinaus zum Einsatz kommen.

Unter einem „Red Team" versteht man in der Cybersicherheit eine Gruppe von Spezialisten, die versucht, in den Kern eines (IT-)Systems vorzudringen. Indem sie Taktiken und Vorgehensweisen von Hackern verwenden, decken diese Spezialisten Schwachstellen auf, die das Unternehmen schließen sollte.

Ähnliche Rahmenwerke gibt es zwar auch in anderen Ländern wie zum Beispiel Großbritannien, dennoch ist das TIBER Rahmenwerk bis jetzt einzigartig auf der Welt. Denn es ermöglicht es mehreren Behörden über Landesgrenzen hinweg, an einer Cyberübung zusammenzuarbeiten. Dahinter steht das Verständnis, dass weder Cyberangreifer noch Akteure auf dem Finanzmarkt ihre Aktivitäten auf einzelne Jurisdiktionen beschränken.

Keine Doppelarbeit

Damit in einem Land überhaupt ein TIBER-Test durchgeführt werden kann, müssen sich erst die zuständigen Behörden (etwa Zentralbank und Bankenaufsicht) zusammenfinden und eine eigene TIBER-Implementierung umsetzen. Dies ist zum Beispiel in den Niederlanden und in Belgien schon geschehen. Ist nun eine Bank in den Niederlanden und in einem weiteren Land wie beispielsweise in Belgien aktiv, so haben die zuständigen Behörden beider Länder die Wahl: Entweder sie führen gemeinsam einen TIBER-Test durch oder sie erkennen den TIBER-Test der jeweils anderen Aufsicht an.

Auf jeden Fall ist sichergestellt, dass der Test nicht doppelt durchgeführt werden muss. Das spart nicht nur Ressourcen, sondern ist auch deutlich sicherer: Ein Red-Team-Test ist ein sehr invasiver Eingriff und legt sensitive Schwachstellen offen. Solche Informationen sollten nicht unnötig repliziert und verteilt werden. Für die Aufsicht reicht oft eine Test-Zusammenfassung, die keine sensiblen Informationen über die konkreten Schwachstellen der Bank preisgibt.

Gründung des Euro Cyber Resilience Boards

Eine weitere Initiative der Notenbanken des Eurosystems ist die Gründung des Euro Cyber Resilience Boards (ECRB). Ziel des ECRB ist es, die Cybersicherheit der europäischen Finanzmarktinfrastrukturen und deren Dienstleister durch eine verbesserte Zusammenarbeit und durch gemeinsame Initiativen zu erhöhen.

Die Mitglieder des ECRB sind Vorstandsmitglieder der größten Finanzmarktinfrastrukturen Europas, denn Cybersicherheit ist ein Thema für die Führungsebene. Zu lange haben sich die Vorstände vieler Unternehmen auf ihre IT-Abteilungen verlassen, wenn es um Cybersicherheit ging. Cybersicherheit ist aber kein reines IT-Thema mehr, sondern eines, mit dem sich die gesamte Organisation beschäftigen muss. Da jeder Mitarbeiter ein Einfallstor für Angreifer darstellen kann, muss entsprechend sensibilisiert werden und eine Unternehmenskultur gelebt werden, in der jeder Mitarbeiter sich seiner Verantwortung bewusst ist.

Zusätzlich zu den Anforderungen und Aktivitäten der unmittelbar beteiligten Akteure im Finanzsektor wird die Cybersicherheit in Europa sektorunabhängig


Foto: F. Rumpenhorst

Johannes Beermann

Mitglied des Vorstands, Deutsche Bundesbank, Frankfurt am Main


Foto: BSI

Arne Schönbohm

Präsident, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Dass Cyberangriffe im privaten wie im öffentlichen Bereich die normalen Abläufe empfindlich stören und große Schäden anrichten können, war auch hierzulande in den vergangenen Jahren für viele Bürger direkt spürbar oder ist ihnen über einschlägige Nachrichten eindringlich vermittelt worden. Auch für die Finanzbranche und dort nicht zuletzt den internationalen Zahlungsverkehr mit seinen langen und komplexen Prozessketten und vielen Akteuren registrieren die Autoren eine Gefährdungslage, die sie durch ein gemeinsames Vorgehen der Markteilnehmer entschärfen wollen. Ermutigende Ansätze zum Aufspüren von Sicherheitslücken und zur Stärkung der Prävention sehen sie im Einsatz von sogenannten Red Teams sowie dem Schutz von kritischen Infrastrukturen durch ein gemeinsames europäisches Rahmenwerk und den regelmäßigen Austausch in internationalen Fachgremien. (Red.)

weiterentwickelt. Die NIS-Richtlinie*, die von den Mitgliedsstaaten der EU bis Mai 2018 in nationales Recht umgesetzt werden musste, ist ein wichtiger Schritt auf dem Weg zu mehr Cybersicherheit in Europa. Der deutsche Gesetzgeber hat seine Hausaufgaben bereits mit der Veröffentlichung des Umsetzungsgesetzes im Juni 2017 erledigt.

Bereits seit Juli 2015 existiert zudem mit dem IT-Sicherheitsgesetz ein einheitlicher Rechtsrahmen für die Zusammenarbeit von Staat und Unternehmen, der Basis für die Umsetzung der NIS-Richtlinie war. Der Rechtsrahmen schreibt Betreibern Kritischer Infrastrukturen vor, IT-Sicherheit nach dem „Stand der Technik" umzusetzen und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Zudem werden im Umsetzungsgesetz die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber Betreibern Kritischer Infrastrukturen erweitert.

Kritische Infrastrukturen im Blick

Ebenfalls im Juni 2017 trat die geänderte BSI-KRITIS-Verordnung in Kraft. Diese bestimmt transparente Kriterien, anhand derer Betreiber Kritischer Infrastrukturen prüfen können, ob sie unter die Regelungen des IT-Sicherheitsgesetzes fallen. Die Verordnung gilt zum Beispiel für die kritischen Dienstleistungen der Bargeldversorgung, des kartengestützten und des konventionellen Zahlungsverkehrs – genau die Bereiche, in denen bedeutende Unternehmen des Finanzsektors aktiv sind. Die registrierten Betreiber Kritischer Infrastrukturen müssen alle zwei Jahre gegenüber dem BSI die Erfüllung der Anforderungen zur Absicherung der Kritischen Infrastrukturen gemäß „Stand der Technik" nachweisen – erstmals im Juni 2019.

Bisher sind spektakuläre Cyberangriffe im Finanzsektor in Europa ausgeblieben. In Deutschland ist die Zahl von etwa zwei Dutzend gemeldeter IT-Sicherheitsvorfälle bei Betreibern Kritischer Infrastrukturen im Finanz- und Versicherungswesen in den ersten fünf Monaten des Jahres überschaubar.

Diese Tatsachen könnten zusammen mit den vielfältigen Anforderungen und Maßnahmen zur Erhöhung der IT-Sicherheit den Eindruck vermitteln, dass Deutschland und Europa gut aufgestellt sind. Und sicher sind die bisher guten Ergebnisse bei der Abwehr von IT-Sicherheitsvorfällen im Finanzsektor in Europa auch das Ergebnis intensiver Bemühungen und guter Arbeit der Beteiligten. Doch ein Stillstand bei der Entwicklung neuer Instrumente der Informationssicherheit ist keinesfalls anzuraten, denn die Gefährdungslage bleibt sehr angespannt.

Zwar können in der Praxis der Beaufsichtigung der Marktteilnehmer und der Überwachung relevanter Finanzmarktinfrastrukturen schon wichtige Erkenntnisse auch zu präventiven Maßnahmen vor Ort erlangt werden. Aber die Betreiber Kritischer Infrastrukturen werden erst Mitte 2019 erstmals Nachweise über ihre jeweiligen Schutzmaßnahmen an das BSI melden. TIBER ist auch noch nicht einsetzbar in Deutschland, denn bis jetzt gibt es noch keine eigene Umsetzung TIBER-DE. Diese gilt es erst noch zu schaffen und bis die ersten Testergebnisse vorliegen, wird noch etwas Zeit ins Land gehen. Daher kann eine Aussage zum notwendigen Aufwand etwa zur Behebung von Mängeln noch nicht getroffen werden.

Unbedarftheit von Nutzern informationstechnischer Systeme

Cybersicherheit muss sehr ernst genommen und prominent auf der Agenda der zu behandelnden Unternehmensrisiken positioniert werden. Dies ist umso wichtiger, als Cyberangriffe heute komplex, vielfältig und mehrdimensional sein können und von professionellen Angreifern durchgeführt werden. Die zunehmende Komplexität, neue technologische Angriffsmöglichkeiten und nicht zuletzt die oft noch zu bemerkende Unbedarftheit von Nutzern informationstechnischer Systeme sind nicht zu unterschätzende Aspekte im Wandel der Bedrohungslage.

Intensiver Austausch auf allen Hierarchieebenen

Die neueren Entwicklungen im Bereich der digitalen Transformation – auch im Finanzsektor – müssen nicht nur mit ihren positiven Verheißungen gesehen werden, sondern auch mit ihrem zusätzlichen Gefahrenpotenzial und ihren Risikofaktoren. Cybersicherheit muss bei der Entwicklung neuer Produkte und Dienstleistungen neben ökonomischen und funktionalen Faktoren berücksichtigt werden (Security by Design). Dies ist eine unverzichtbare Voraussetzung für das Gelingen der Digitalisierung. Auch Datenschutz kann nur vernünftig umgesetzt werden, wenn die Informationssicherheit gewährleistet ist.

Nicht nur in der Überwachung und Aufsicht im Finanzsektor, sondern auch in der Kommunikation mit der Wirtschaft wird immer wieder betont, dass im Kampf gegen Cyberrisiken eine Kooperation aller Beteiligten notwendig ist. Dies bezieht auch die jeweils zuständigen Behörden mit ein.

Die Deutsche Bundesbank und das BSI haben bereits in der Vergangenheit bewiesen, dass eine solche Kooperation durch intensiven Austausch auf allen Hierarchieebenen möglich und nutzbringend ist. Das BSI und die Deutsche Bundesbank werden nach Kräften in Konsultationen und gemeinsamen Initiativen dazu beitragen, dass der deutsche Finanzsektor sich für die Bedrohungen der Zukunft wappnen kann.

* Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union