Arne Schönbohm

Cyberresilienz im Finanzsektor

Die Digitalisierung steht als Synonym für schnell fortschreitende, technische Innovationen, die auf unterschiedliche Weise mit dem Thema der Informationssicherheit verknüpft sind. Technische Entwicklungen, etwa im Bereich der Automobilindustrie, der Mobilkommunikation oder im Internet der Dinge, werfen die Frage auf, wie sicher solche Systeme vor externer Einflussnahme sind. Betrachtet man die Aktivitäten und Zahlen im Bereich der Digitalisierung, muss man feststellen, dass die Digitalisierung erst begonnen hat.

Heute ist viel von Themen wie Industrie 4.0, von Smart Factory und Smart Services oder vom Stichwort vernetzte Autos zu lesen und zu hören. Schon vor Jahren hat der Altministerpräsident in Hessen, Roland Koch, vom staufreien Hessen gesprochen, mit dem autonomen Fahren rückt diese Vision nun näher. Um all das zu erreichen, werden Technologien benötigt wie beispielsweise eine Blockchain, künstliche Intelligenz – wobei es eigentlich um das Thema des maschinellen Lernens geht – und Quantencomputer. Die quantenresistente Verschlüsselung ist übrigens ein Thema, das alle noch intensiv beschäftigen wird.

Informationssicherheit als Voraussetzung der Digitalisierung

Die spannende Herausforderung ist, wie diese unabwendbare technologische Entwicklung in Zukunft verläuft, wie ihre Chancen und wie ihre Risiken eingeschätzt werden. Wenn genauso weiter digitalisiert wird wie in der Vergangenheit, dann wird dieser Kampf im Bereich der Informationssicherheit verloren. Informationssicherheit ist dabei keineswegs der Kostenfaktor, während die Digitalisierung der Ertragsbringer ist, sondern Informationssicherheit ist die Voraussetzung der Digitalisierung, sie ist deren zentrales Element. Es kann nur dann digitalisiert werden, wenn es sicher funktioniert. Keiner wird ein Bankgeschäft machen oder Geld überweisen, wenn er nicht sicher sein kann, dass das Geld auch dort hingeht, wo es hingehen soll, oder wenn er befürchten muss, dass eine Blockchain missbraucht wird. Solche Vorfälle sind bekannt. Zu dieser Thematik hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) gerade gemeinsam mit der BaFin ein Konzeptpapier veröffentlicht.

Bei all diesen neuen Technologien ist es ganz entscheidend, auch die Risiken mit zu bedenken und dann eine bewusste Entscheidung zu treffen. Welche Risiken sollen eingegangen werden und welche nicht? Um diese Frage dreht sich auch die aktuelle Diskussion zum Thema 5G-Netzaufbau in Deutschland und die Einbindung des chinesischen Anbieters Huawei in dieses Projekt. An dieser Stelle muss sich die Bundesregierung positionieren, welche Risiken sie einzugehen bereit ist und welche nicht. Vor ähnlichen Problemen stehen alle Entscheider in der Wirtschaft, auch in den Banken. Das ist Chefsache. Niemand kann sich darauf zurückziehen, dass der IT-Verantwortliche, der Chief Security Officer oder der CIO das schon regelt. Informationssicherheit muss jeder Entscheider verstehen. Auf dieser Basis ist es dann seine Aufgabe zu sagen, welche Risiken er einzugehen bereit ist, und wie die Risiken zu managen sind. Diese Grundthematik wird nicht verschwinden, sondern eher an Bedeutung gewinnen, weil die Abhängigkeit von der IT ständig steigt.

Ein Anschauungsbeispiel für Cyberrisiken in der IT liefert seit rund zwei Jahren der Fall der dänischen Reederei Maersk, der immer wieder von den Medien aufgegriffen wird. Durch einen Ransomware-Angriff mit Not-Petya, einer ähnlichen Schadsoftware wie sie einen Monat zuvor auch beim sogenannten Wannacry-Angriff auf viele Großkonzerne und öffentliche Einrichtungen eingesetzt worden war, wurden die Computersysteme von Maersk zeitweise lahmgelegt. Die Computer-Infrastruktur musste neu aufgesetzt werden, der Schaden wird auf bis zu 300 Millionen Dollar veranschlagt.

Bedrohungslage

Spätestens an dieser Stelle dürfte sich auch jeder Verantwortliche im Bereich Kreditwürdigkeitsprüfung der Banken fragen, wie sicher Maersk im Bereich der IT aufgestellt ist. Und dieses Beispiel lässt sich natürlich auf alle kreditgebenden Banken und ihre Kunden übertragen. Die Verantwortlichen in den Banken müssen das Thema der Digitalisierung verstehen, um die Risiken ihrer Kunden vernünftig einschätzen zu können und selbst als Bank ein gutes Risikomanagement machen zu können.

Früher hatte man von einem Hacker ein fast schon idyllisches Bild. Mit einem Kapuzenpullover, Pizza essend und Cola trinkend sitzt er im Keller und plündert mit dem Smartphone tatsächlich das Konto der Großmutter oder des Großvaters. Das ist leider nicht mehr so. Heute gibt es

Arne Schönbohm

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

In allen Bereichen des gesellschaftlichen und wirtschaftlichen Lebens übt die Welle der Digitalisierung gleichermaßen Faszination und Erstaunen aus und steht dennoch erst am Anfang. Als zentrale Voraussetzung einer erfolgreichen Digitalisierung sieht der Autor allerdings zwingend die Informationssicherheit und gibt an Zahlen- und Fallbeispielen einen Einblick in die Bedrohungslage der Cyberrisiken. Beim Einsatz neuer Technologien hält er es für entscheidend, stets die Risiken mit zu bedenken und dann eine bewusste Entscheidung zu treffen. Sein Haus hat als nationale Cybersicherheitsbehörde und Kompetenzzentrum mit der Wirtschaft und in Zusammenarbeit mit Betreibern kritischer Infrastrukturen eine Allianz aufgebaut, um auf Basis von Wissen und Fakten branchenspezifische Sicherheitsstandards zu erarbeiten. Mit Blick auf die Finanzwirtschaft betont er die Zusammenarbeit mit der Bundesbank, beispielsweise bei der Geldabwicklung, die die Übertragung der Daten und der Geldströme vertrauensvoll, gut, schnell und vernünftig sicherstellen muss. (Red.)

jeden Tag knapp 400 000 neue Schadprogramme. Weltweit ist von 800 Millionen Schadprogrammen auszugehen. Das Schadenspotenzial wird auf 50 Milliarden Euro jährlich allein für die deutsche Wirtschaft veranschlagt. Seit 2009 verdient die organisierte Kriminalität mehr Geld mit Cybercrime als mit Drogen.

Es ist aber nicht nur über Cyberangriffe mit Schadprogrammen (Malware, DDoS-Angriffe) zu reden, sondern auch über erhebliche herstellerseitige Lücken in der Software. Konkret gibt es allein rund 700 Lücken in den zehn am meisten verbreiteten Software-Programmen. Man hat sich an solche Lücken gewöhnt, die nicht entsprechend geschlossen werden. Aber wenn sie einmal in einem Programm enthalten sind, migrieren sie weiter in verschiedene Systeme. Und das ist nicht alles. Auch bei der Hardware sind Lücken festgestellt worden, etwa bei Chips. Im vergangenen Jahr und Anfang dieses Jahres haben Wissenschaftler die Chip-Risiken untersucht und konnten dabei Sicherheitslücken nachweisen.

Zunehmend lässt sich aufgrund der Komplexität der Produkte der Informationstechnik schwieriger abschätzen, wie sicher ein Produkt ist. Auch die Frage, ob und in welche Produkte Sicherheitslücken von vornherein eingebaut sind und in welche nicht, ist eine Herausforderung. Diesen Fragen müssen sich alle Beteiligten stellen.

Das BSI als nationale Cybersicherheitsbehörde

Der Bund hat das BSI, das Bundesamt für Sicherheit in der Informationstechnik, vor knapp 30 Jahren gegründet. Noch vor wenigen Jahren führte diese Behörde ein Schattendasein. Das hat sich geändert. Mit der rasant fortschreitenden Digitalisierung aller Lebensbereiche, mit der wachsenden Zahl von Cyberangriffen ist auch die Bekanntheit des BSI gewachsen. Es hat 2015 durch das IT-Sicherheitsgesetz neue Aufgaben und mehr Verantwortung bekommen.

Vor etwas über drei Jahren hat das BSI darum einen Leitspruch entwickelt und klar betont, wofür es eigentlich steht und was es will: Als die nationale Cybersicherheitsbehörde gestaltet das BSI Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. In den USA gibt es eine hohe zweistellige Zahl von Institutionen, die für das Thema Cybersicherheit zuständig sind. Es gibt die zum Beispiel die NSA, es gibt die Cybersecurity and Infrastructure Security Agency (CISA) im Department of Homeland Security, es gibt die National Cyber Security Division (NCSD). Alle arbeiten in verschiedenen Bereichen. Wenn man allen diesen Institutionen sagt, es muss die Cybersicherheit vorangetrieben werden, dann werkelt jeder ein bisschen herum. Das BSI hingegen weiß ganz genau, was zu tun ist und das passiert dann auch. Das ist der Vorteil einer nationalen Cybersicherheitsbehörde. Sie ist das Kompetenzzentrum.

Das heißt natürlich nicht, dass man alles alleine macht, sondern man unterstützt die anderen Einrichtungen und Behörden als Kompetenzzentrum. Darum baut das BSI sein Know-how weiter aus, beispielsweise im Bereich des maschinellen Lernens. Darum hat es bei der Hardware-Sicherheitskonferenz CHES 2018 (Cryptographic Hardware and Embedded Systems), der Olympiade des maschinellen Lernens, an zwei Einzeldisziplinen des Kryptowettbewerbs „CHES 2018 Challenge“ teilgenommen, hat die reale Intelligenz mit der künstlichen Intelligenz gepaart und hat dabei in beiden Disziplinen gewonnen. Auf diese Kompetenz des BSI können die Institutionen in Staat, Wirtschaft, Gesellschaft zugreifen. Das ist der Grundgedanke, mit dem der Satz „Netzwerke schützen Netzwerke“ mit Leben erfüllt wird. Damit wird gemeinsam Informationssicherheit in der Digitalisierung gestaltet.

Die zentrale Stelle für Informationssicherheit

Das BSI ist die zentrale Stelle für Informationssicherheit in Staat, Wirtschaft und Gesellschaft. Zentrale Aufgabe ist der Schutz der Bundesregierung. Das BSI ist nicht zuständig für den Bundestag, weil das Parlament die Regierung kontrolliert. Aber es arbeitet auch mit dem Bundestag und der Bundestagsverwaltung eng und vertrauensvoll zusammen.

Was machen die Bundesländer? Im föderalen Staat ist natürlich jedes Land für seine eigene IT-Sicherheit verantwortlich, aber als Kompetenzzentrum unterstützt das BSI auch die Bundesländer. Dazu wurden in den vergangenen Monaten mit

neun Ländern Absichtserklärungen unterschrieben für eine bessere Versorgung und für einen besseren Austausch im Bereich der Informationssicherheit.

So wurde eine Malware-Information-Sharing-Plattform aufgebaut. Denn auch die Bundesländer können und sollen wissen, welche Angriffssignaturen das BSI hat, damit sie mit diesen Erkenntnissen schnell und wirkungsvoll ihre eigenen Schutzmaßnahmen gegen Cyberangriffe gestalten können. Mit Ausnahme einiger wenigen vertraulich oder geheim eingestuften Signaturen sind diese Angriffssignaturen auch anderen Akteuren in Wirtschaft und Gesellschaft zugänglich.

Allianz für Cybersicherheit

In der Wirtschaft hat das BSI eine Allianz für Cybersicherheit mit knapp 4000 Unternehmen aufgebaut sowie den UP KRITIS, wo Betreiber kritischer Infrastrukturen vertrauensvoll mit dem BSI zusammenarbeiten. Dort werden branchenspezifische Sicherheitsstandards erarbeitet – erst kürzlich für das Thema Ernährung und Landwirtschaft. Und auch mit gesellschaftlichen Institutionen wie den Verbraucherzentralen arbeitet das BSI eng zusammen. Es entwickelt zum Beispiel ein sogenanntes IT-Sicherheitskennzeichen, für Handys, für Router und andere IT-Produkte. Derzeit haben Verbraucher kaum eine Chance zu erkennen, wie sicher ihr Smartphone ist. Es wurden sogar Plagiate verkauft, auf denen eine Schadsoftware schon als Service installiert war. Deshalb arbeitet das BSI daran, mit dem IT-Sicherheitskennzeichen dem Verbraucher eine Orientierung zu geben, damit er bewusst entscheiden kann, welche Risiken er eingehen will und welche nicht.

Eine ganz wichtige Diskussion betrifft den Stand der Technik, der zur Absicherung kritischer Infrastrukturen von Betreibern eingehalten werden soll und damit Beiträge zur Resilienz im Finanzsektor liefert. An dieser Stelle gibt es eine enge Zusammenarbeit und einen vertrauensvollen Austausch mit der Deutschen Bundesbank und ebenso mit der BaFin. Als starkes Team wird über aktuelle Themen diskutiert und beraten. Auf dieser Basis werden dann die richtigen Maßnahmen eingeleitet, und zwar immer auf Basis von Fakten und nicht in gutem Glauben. Wie sehr beides verschwimmen kann, zeigt ein Erlebnis beim Besuch eines großen Unternehmens. Dort wurde dem BSI eben noch auf Präsentationsfolien dargestellt, was alles im Bereich der Cybersicherheit unternommen wird. Aber schon beim Verlassen des Werksgeländes kam auf dem dienstlichen Smartphone eine verschlüsselte Nachricht an, dass just dieses Unternehmen gerade angegriffen worden ist.

Die klare Erkenntnis und Botschaft dieser Begebenheit war wieder einmal: Das BSI als nationale Cybersicherheitsbehörde kann und darf sich nicht auf den Glauben verlassen, sondern muss auf Fakten und Wissen bauen. Es will sicherheitsrelevante Sachverhalte gerne wissen, um den Betroffenen Unterstützung anbieten und gewähren zu können, nicht um sie an den Pranger zu stellen. Die Systeme in der Zahlungsabwicklung beispielsweise sollen möglichst so gehärtet sein, dass sich die Risiken minimieren lassen. Dem dienen auch verschiedene Maßnahmen, beispielsweise der gemeinsame Brief mit dem BaFin-Präsidenten Felix Hufeld im August 2018 zum Thema bankaufsichtliche Anforderungen an die IT kritischer Infrastrukturen, in dem die Vorstellungen beider Häuser dementsprechend dokumentiert wurden.

Zusammenarbeit mit der Bundesbank

Auch die Zusammenarbeit zwischen der Deutschen Bundesbank und dem BSI ist auf einem guten Weg. Beispielsweise sei der Austausch zur nationalen Umsetzung des TIBER-Frameworks (Threat-Intelligence based Ethical Red Teaming) genannt. Es geht nicht nur um die Banken als Opfer von Cyberattacken. Auch die Bewertung der Risiken der Bankkunden ist eine ganz zentrale Fragestellung. Die Bewertung der Kreditwürdigkeit für Unternehmen wird immer stärker davon beeinflusst, wie deren IT aufgestellt ist, ob sie gegen Angriffe versichert ist, welche Mindestmaßnahmen getroffen wurden, um die Bedrohungslage einzuschätzen und die Risiken gegebenenfalls anders zu managen. All diese Themen sollte man nicht allein, sondern gemeinsam angehen.

Ohne Cybersicherheit wird die Digitalisierung nicht erfolgreich verlaufen. Es gibt viele Fälle, in denen die Themen Sicherheit und Funktionalität nicht richtig berücksichtigt wurden. Ein schönes Beispiel liefert der beeindruckende Wachstumsprozess von Amazon und dessen Philosophie für den Umgang mit Innovationen. Ein Punkt ist dabei hochinteressant. Etwas Innovatives, etwas Neues, etwas Sicheres zu machen beginnt dort mit einer Presseerklärung. Warum? Eine Presseerklärung enthält Aussagen, was in welcher Zeit erreicht werden soll und welchen Mehrwert es für die Kunden bringt. Als größter Flop gilt in dem Unternehmen bezeichnenderweise das Telefon Amazon Fire, und zwar nicht, weil es sich schlecht verkauft hätte, sondern weil es bei Millionen Kunden nach zwei Monaten in der Schublade verschwunden ist. Mit dem Misserfolg des Telefons am Markt, so die Sicht von Amazon, wurde viel von dem gesamten Image, das an anderer Stelle aufgebaut worden ist, kaputt gemacht.

Kunden arbeiten mit Unternehmen zusammen, weil sie Vertrauen haben. Genau das ist deren Kapital. Und genau aus diesem Grund muss auch bei der Geldabwicklung die Übertragung der Daten und der Geldströme absolut vertrauensvoll, gut, schnell und vernünftig funktionieren. Dafür sind die Finanzdienstleister da. Digitalisierung ist ein Hilfsmittel, die Abwicklung besser und effizienter zu machen, aber am Ende stehen die Finanzdienstleister mit ihrem guten Namen dafür ein, das es sicher funktioniert. Das BSI will die Branche gerne dabei unterstützen, die Digitalisierung gemeinsam erfolgreich zu gestalten.

Der Beitrag basiert auf einer Rede des Autors anlässlich des Bundesbank-Symposiums „Zahlungsverkehr und Wertpapierabwicklung in Deutschland im Jahr 2019“ am 29. Mai 2019 in Frankfurt am Main.

Die Zwischenüberschriften sind teilweise von der Redaktion eingefügt.