Sustainable Cyber Resilience im Finanzsektor:

Finanz- und Versicherungswesen

Whitepaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

09/2018

Management Summary

Banken, Börsen, Versicherungen und Finanzdienstleister zählen zu den kritischen Infrastrukturen und sind ein attraktives Ziel für Hacker. Um für angemessenen Schutz zu sorgen, reicht es nicht mehr aus, reaktive Maßnahmen zu ergreifen. Stattdessen müssen Unternehmen einen Zustand der Sustainable Cyber Resilience anstreben: der nachhaltigen Widerstandsfähigkeit. Dabei handelt es sich um ein umfassendes Konzept, das eher strategisch als technologisch ausgerichtet ist und einen Schritt weiter geht als IT Security. Sustainable Cyber Resilience sorgt zum einen dafür, Angriffsflächen zu verringern. Zum anderen stellt sie sicher, dass Unternehmen ihren Betrieb auch im Falle eines Angriffs aufrechterhalten und ihre angestrebten Geschäftsziele erreichen können – unter Berücksichtigung der Wirtschaftlichkeit. Dieses Whitepaper zeigt, warum Sustainable Cyber Resilience für den Finanzsektor so wichtig ist, was sie bedeutet und wie sie sich mithilfe von Vulnerability Management umsetzen lässt.

Inhalte

Einleitung

Sustainable Cyber Resilience ist für Unternehmen aller Branchen wichtig. Unverzichtbar ist sie aber im Bereich der kritischen Infrastrukturen (KRITIS). Darunter fallen laut Definition der Bundesregierung „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." KRITIS-Organisationen müssen sich daher besonders gut gegen Cyber-Angriffe schützen – das schreibt der Gesetzgeber vor. Die EU begann bereits 2006 mit dem European Programme for Critical Infrastructure Protection (EPCIP) und erweiterte und ergänzte dieses in den folgenden Jahren. Mitgliedsstaaten setzen die EU-NIS Direktive in nationales Recht um, Deutschland beispielsweise mit dem IT-Sicherheitsgesetz (IT-SIG). Große Wirtschaftsnationen haben bereits Regulierungsinstanzen entwickelt. In den USA ist dies zum Beispiel das US National Institute of Standards and Technology und in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI).

In Deutschland sind die kritischen Infrastrukturen in 9 Sektoren eingeteilt. Einer davon ist das Finanz- und Versicherungswesen. Es umfasst Banken, Börsen, Versicherungen und Finanzdienstleister. Sie spielen eine entscheidende Rolle für unsere moderne Gesellschaft. Ohne einen funktionierenden Zahlungsverkehr käme der gesamte Handel zum Erliegen. Wir könnten keine Lebensmittel mehr einkaufen und würden keine Gehälter mehr erhalten. Banken sorgen dafür, dass wir Geld sicher aufbewahren, abheben oder überweisen können. Versicherungen dienen uns als Altersvorsorge oder erbringen finanzielle Leistungen im Schadensfall. Der Staat braucht den Finanzsektor, um Steuerzahlungen von Bürgern und Unternehmen zu beziehen oder Anleihen zur eigenen Refinanzierung zu platzieren.

Für Cyber-Kriminelle sind Unternehmen aus dem Finanz- und Versicherungswesen ein attraktives Ziel, weil sie hier direkt Geld erbeuten können, ohne dass sie erst anderes Diebesgut verkaufen müssen. So ist es nicht verwunderlich, dass der Finanzsektor laut einer Studie von Dimension Data die am häufigsten angegriffene Branche ist. Wie eine Umfrage des Sicherheitsspezialisten Kaspersky zeigt, war mehr als jede vierte Finanzorganisation bereits Opfer von zielgerichteten Attacken und Malware-Vorfällen. 70 Prozent der Banken hatten Finanzbetrügereien mit Geldverlust ihrer Kunden zu beklagen. Dabei lag der Schaden durchschnittlich bei 1.466 US-Dollar für Privat- und 10.312 US-Dollar für Geschäftskunden. Ihres erhöhten Risikos sind sich Unternehmen aus dem Finanzsektor durchaus bewusst. So geben sie dreimal so viel für Cyber-Sicherheit aus wie Organisationen aus anderen Branchen.

Beispiele für Cyber-Attacken auf Infrastrukturen des Finanzsektors

In den vergangenen Jahren gab es weltweit zahlreiche Angriffe auf kritische Infrastrukturen im Finanzsektor. So attackierten Hacker im Sommer 2014 die amerikanische Bank J.P. Morgan und stahlen Daten von über 76 Millionen Privat- und sieben Millionen Geschäftskunden. Die Datensätze umfassten neben Name, Adresse, Telefonnummer und E-Mail-Adresse auch bankinterne Informationen der Kunden. Offensichtlich waren die Angreifer äußerst gewieft. Für ihren Hack nutzten sie eine Zero-Day-Schwachstelle aus, eine Sicherheitslücke, die bis dahin unbekannt war. Sie infizierten die IT-Systeme der Bank mit einer eigens dafür programmierten Schadsoftware, die es ihnen ermöglichte, die Systeme fernzusteuern. Erst zwei Monate später entdeckte J.P. Morgan den Vorfall.

Im Februar 2016 erbeuteten Cyber-Kriminelle in einem spektakulären digitalen Bankraub 81 Millionen US-Dollar. Sie hatten sich in das SWIFT-System der Zentralbank von Bangladesch gehackt und Beträge im Wert von einer Milliarde US-Dollar an die US-Notenbank Fed gesendet. Die Angreifer nutzten für ihren Coup eine hochspezialisierte Malware, die Sicherheitsexperten zufolge speziell für diesen Zweck programmiert worden war. SWIFT ist ein globales Bank-Messaging-System, mit dem Banken Nachrichten zum Zahlungsverkehr austauschen, zum Beispiel Überweisungsaufträge. Wie die Nachrichtenagentur Reuters berichtete, kam es im Februar 2018 erneut zu ähnlichen Vorfällen. Die indische City Union Bank hatte festgestellt, dass ihre Systeme gehackt und 1,5 Millionen Euro unautorisiert an internationale Banken überwiesen wurden. Auch die russische Zentralbank erklärte, dass ihr über das SWIFT-System 4,8 Millionen Euro gestohlen worden seien.

Gleich zweimal wurde die italienische Großbank Unicredit Opfer einer Cyber-Attacke. Hackern gelang es, in die Datenbanken des Unternehmens einzudringen und sich Zugriff auf Kreditinformationen von rund 400.000 Kunden zu verschaffen. Die Angriffe ereigneten sich zwischen September und Oktober 2016 sowie erneut im Juni und Juli 2017.

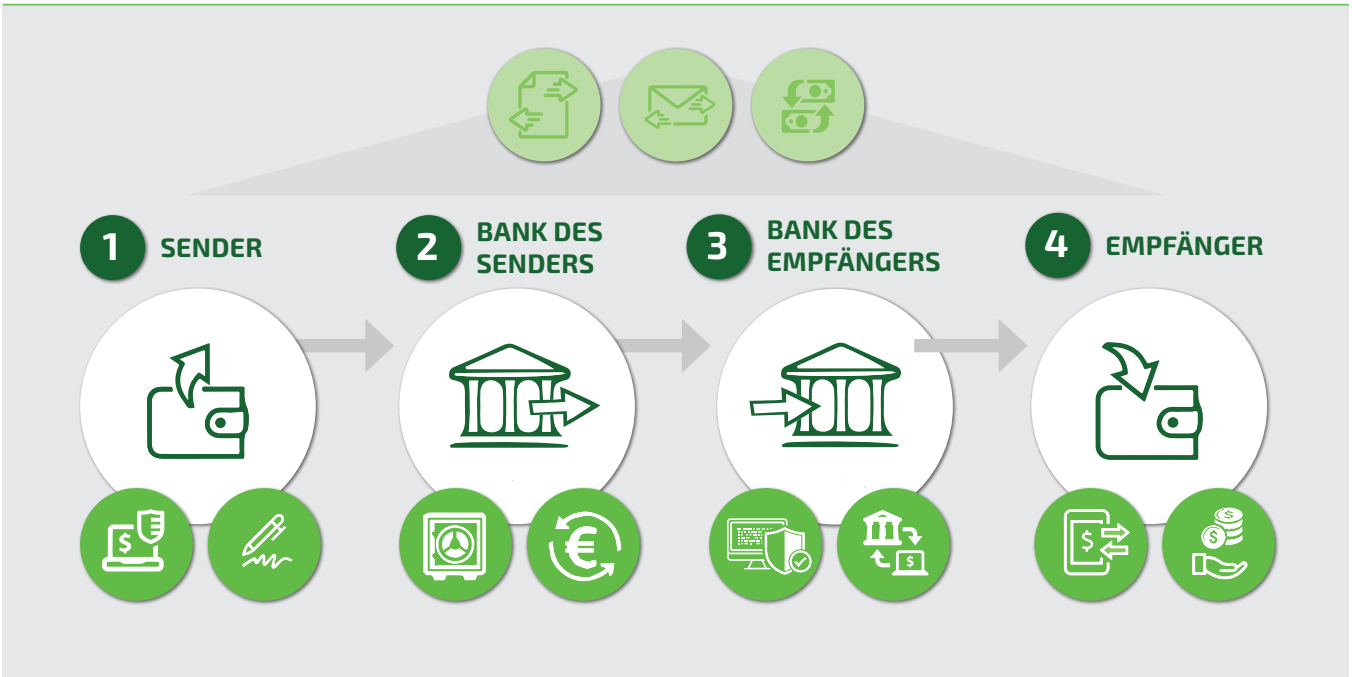
Einen Coup von bisher nie dagewesenem Ausmaß in der Finanzbranche erlitt die Wirtschaftsauskunftei Equifax. Im Mai 2017 gelang es Hackern, in die Systeme des größten amerikanischen Credit Bureaus einzudringen und Daten von mehr als 143 Millionen US-Bürgern zu stehlen, darunter Kreditkarten- und Sozialversicherungsnummern. Die Auskunftei sammelt Daten zum Finanzgebaren von Verbrauchern und errechnet daraus Kennzahlen, die sie dann an potenzielle Vermieter oder Arbeitgeber verkauft. Für den Angriff nutzten die Hacker eine Sicherheitslücke im Open-Source-Framework Apache Struts aus. Diese war bereits seit Anfang März bekannt. Equifax hatte den entsprechenden Patch jedoch nicht eingespielt.

IT-Systeme und Prozesse im Finanzsektor

Die Abläufe in der Finanzwelt sind etwas vereinfacht in der Grafik unten dargestellt. Der Sender (1) einer Transaktion erfasst die dazu notwendigen Daten und identifiziert sich selbst, zum Beispiel über TAN-Verfahren oder durch digitale Signaturen. Die Bank des Senders (2) prüft die Identität, verifiziert die Daten der Transaktion (Limits der Transaktion, des Kontos, der Person) und übermittelt sie an die empfangende Bank (3). Diese wiederum überprüft und verifiziert diese Daten ebenfalls, um sie dann dem Empfänger (4) gutzuschreiben. Alle Kommunikationsabläufe nutzen kryptografische Verfahren, deren Validität und Schlüssellänge stets überprüft werden müssen.

Unternehmen im Finanz- und Versicherungswesen arbeiten heute medienbruchfrei mit digitalen Dokumenten und weitgehend automatisierten Workflows. Dadurch sind sie auch gut auf digitalem Weg angreifbar. Zu den wichtigsten Zielen für Hacker zählen neben Office- und E-Mail-Systemen, Unternehmensnetzwerken und Datenbanken vor allem buchführende IT-Systeme und ihre vorgelagerten Anwendungen, Steuerungs- und Controlling-Anwendungen, Systeme für Risikomanagement und Risikoberichterstattung, Zahlungsverkehrssysteme, Handelssysteme sowie Schnittstellen zu Kunden und Geschäftspartnern wie Kundenportale, Apps oder Geldautomaten. Um einen Zustand der Sustainable Cyber Resilience zu erreichen, müssen Unternehmen des Finanzsektors das gesamte Spektrum der vernetzten Systeme, Geräte und Applikationen berücksichtigen.

IT-basierende Transaktionen im Finanzwesen



Buchführenden Systeme kommen zum Einsatz, um Konten und Depots zu verwalten und Transaktionen durchzuführen. Ihnen sind IT-Anwendungen vorgelagert, die Geschäftsprozesse umsetzen. Sie steuern in automatisierten Workflows Aktivitäten, generieren Kennzahlen oder veranlassen Kontrollen. Gelingt es Cyber-Kriminellen in die vorgelagerten Systeme oder die buchführenden Systeme einzudringen, könnten sie zum Beispiel Kontobewegungen oder Depotstände verändern.

Handelssysteme leiten Orders an die Börse weiter. Oft kommen auch intelligente Algorithmushandelssysteme zum Einsatz, die automatisiert die optimale Stückelung der Orders erzeugen. Für Cyber-Kriminelle ist es attraktiv, Handelsdaten auszuspähen, denn damit können sie Insider-Handel vorbereiten. Außerdem hätten sie die Möglichkeit, die Order-Weiterleitung zu verzögern und sich dadurch einen Handelsvorteil zu verschaffen.

Besondere Herausforderungen für Resilience im Finanzsektor

Unternehmen aus der Banken- und Versicherungsbranche stehen durch die Digitalisierung unter großem Druck. Fintechs graben ihnen mit innovativen Geschäftsmodellen den Markt ab. Gleichzeitig steigen die Erwartungen der Kunden, die sich eine bessere Customer Experience und neue, mobile Services wünschen. Um Bestandskunden bei der Stange zu halten und neue Kundengruppen zu erschließen, müssen Banken und Versicherungen sich auf unbekanntes Terrain vorwagen. Während sie bisher nur die IT im eigenen Haus absichern mussten, entstehen jetzt neue Risiken durch mobile Endgeräte, Apps und Webanwendungen, die auf vielfältige Weise verwundbar sind. Dabei vergrößert die zunehmende Vernetzung mit Kunden und anderen Finanzdienstleistern die Angriffsfläche.

Zudem lagern Banken und Versicherungen heute IT-Dienstleistungen wie die Softwareentwicklung häufig an externe Anbieter aus. Wie der Bafin-Leiter für IT Sicherheit feststellte, hat sich die Zahl der Dienstleister in diesem Bereich jedoch stark reduziert. Wenn dieselben Entwickler für viele Banken arbeiten, können sich Programmierfehler oder Sicherheitslücken aber auch schneller über das gesamte Bankenwesen verbreiten.

Erschwerend kommt hinzu, dass Unternehmen aus dem Finanzsektor zahlreiche nationale und internationale Regularien erfüllen müssen. Sie alle formulieren Anforderungen an die IT Security und das Risikomanagement. Das macht es komplex, ein umfassendes IT Security und Resilience-Konzept zu entwickeln. Als gemeinsamer Baustein wird jedoch Vulnerability Management in vielen Richtlinien explizit als Sicherheitsmaßnahme genannt.

Vulnerability Management als wichtiger Baustein für Sustainable Cyber Resilience

Resilienz ist ein kontinuierlicher Prozess. Er verstärkt die Fähigkeit eines Unternehmens, einer Attacke zu widerstehen, und versetzt es in die Lage, auch während eines Angriffs zu funktionieren. Um dies zu erreichen, ist es wichtig, die Angriffsfläche zu reduzieren und so die Basis zu stabilisieren. Das bedeutet, Schwachstellen zu identifizieren, die von einem Angreifer ausgenutzt werden könnten. Letztlich heißt es, dem Angreifer einen Schritt voraus zu sein.

Greenbones Schwachstellenmanagement funktioniert mit dem Greenbone Security Manager (GSM) und ist dafür gedacht, Resilience durch einen kontinuierlichen Prozess nachhaltig zu etablieren. Dieser besteht aus den folgenden, größtenteils automatisierten Schritten:

Prepare

Im ersten Schritt geht es darum, den Kontext zu IT-Sicherheits-Policies, Risikobewertungen, Unternehmensprozessen und unternehmenskritischen Systemen herzustellen. Was will ich wie und wie intensiv schützen? Wie viel Risiko bin ich bereit zuzulassen? In Konfigurationsrichtlinien legen die IT-Verantwortlichen fest, was im Rahmen der Sicherheitsvorgaben erlaubt ist. Diese Richtlinien können dann mit einer technischen Kontrolle im GSM verknüpft werden. Hinzu kommen Informationen rund um den Security Workflow und die Verantwortlichkeiten. Wer muss informiert sein? Wer entscheidet, ob eine Schwachstelle behoben werden soll oder darf? Wer behebt sie?

Identify

Jetzt folgt die Analyse der Ist-Situation. Ein Vulnerability Scan stellt fest, welche Schwachstellen die Infrastruktur

aktuell aufweist und wo sie von Konfigurationsvorgaben abweicht. Dabei muss sichergestellt werden, dass die Datenbank mit den Schwachstelleninformationen auf dem neuesten Stand ist. Außerdem wird identifiziert, wo genau sich die Schwachstelle oder Abweichung von der Norm befindet, und hinterfragt, wie belastbar die gefundenen Ergebnisse sind. Das dient dazu, False Positives und False Negatives zu vermeiden. Greenbone hat dafür das Feature QoD „Quality of Detection“ eingebaut. Es nennt einen Prozentwert, mit welcher Wahrscheinlichkeit die Schwachstelle tatsächlich existiert.

Classify

Die gesammelten Informationen werden jetzt nach unterschiedlichen Kriterien eingeteilt, die das Unternehmen individuell festlegen kann – zum Beispiel wo ein System physikalisch steht, zu welcher Abteilung es gehört, in welchem Netzsegment es sich befindet und welche Funktion es im Unternehmen erfüllt. Diese Einteilung ist unabhängig von der Kritikalität der Schwachstelle. Classify macht nichts anderes, als die Funde anhand der vorhandenen Merkmale zu gruppieren. Wichtig hierbei ist, dass eine solche Gruppierung im Sinne der Automatisierung in Regeln abgebildet werden kann.

Prioritize

Jetzt wird priorisiert, was auf Basis der Ziele aus dem ersten Schritt „Prepare“ mit den gefundenen Schwachstellen aus dem Schritt „Identify“ anhand der Einteilungen von „Classify“ am wichtigsten und damit als Erstes zu tun ist. Welcher Fund hat die größte Auswirkung und muss zuerst bearbeitet werden?

Assign, Mitigate & Remediate

Die technischen Erkenntnisse müssen in einem Arbeitsprozess münden, der zur Schließung der Schwachstelle führt. Ein Vulnerability-Management-Prozess sollte regeln, wer wann welche Informationen zu entdeckten Schwachstellen bekommt, wer für welche Schritte verantwortlich ist und welche Mittel und Wege zur Verfügung stehen. Das Vulnerability-Management-System sollte hier so viele Informationen wie nur möglich mitliefern. Die Handlung kann auch über den Austausch mit anderen Workflow Tools initiiert werden, zum Beispiel einem ISMS, einem Ticket-System

Widerstandsfähigkeit durch den Schwachstellen-Management-Prozess

für Helpdesks oder einem SIEM-System zur weiteren Korrelation von Security Events beziehungsweise Incidents.

Store & Repeat, Improve

Die letzten Schritte dienen der Auditierbarkeit des Systems nach ISO 27000 sowie der Verbesserung, Veränderung und Anpassung. Store & Repeat protokolliert wichtige Informationen, zum Beispiel, wann eine Schwachstelle zum ersten Mal gefunden wurde, wann sie gemeldet wurde und wie lange es gedauert hat, sie zu beheben. Dies hilft bei der Analyse von Sicherheitsvorfällen. „Improve“ ist der Übergang zu einem erneuten Durchlauf des Vulnerability-Management-Prozesses, der wieder mit „Prepare“ beginnt. Jetzt können Sicherheitsverantwortliche die Zielsetzung verfeinern, verschärften oder an veränderte Policies anpassen. Schwachstellenmanagement ist kein statisches System, sondern ein dynamischer Prozess, bleibt aber immer automatisierbar.

Grenzen von Vulnerability Management

Vulnerability Management ist ein wichtiger Baustein, um Sustainable Cyber Resilience zu erreichen. Es ist jedoch nur ein Element in einer umfassenden Gesamtarchitektur. Für nachhaltige Cyber Security und Widerstandsfähigkeit sind noch viele weitere Faktoren zu berücksichtigen, die ineinandergreifen müssen. Neben der Absicherung der Systeme gegen Hacker-Angriffe dürfen Unternehmen auch die physische Sicherheit nicht vernachlässigen. Zudem spielen organisatorische Maßnahmen eine wichtige Rolle. Unternehmen müssen genau festlegen und dokumentieren, wie Security-Prozesse aussehen und wer welche Aufgaben und Verantwortung übernimmt. Außerdem dürfen Unternehmen den Faktor Mensch nicht vergessen. Eine wichtige Präventionsmaßnahme sind nach wie vor Schulungen zur Sensibilisierung für IT-Risiken. Denn viele Mitarbeiter sind sich nicht bewusst, wie gefährlich Fehlverhalten oder Unachtsamkeit sein kann.

Nicht umsonst schreiben zahlreiche Richtlinien und Gesetze Schwachstellen-Scans und Risikobewertung vor. So erwartet zum Beispiel die EU-DSGVO ein implementiertes Schwachstellenmanagement. Auch für eine ISO 27001-Zertifzierung ist dies Voraussetzung. Die Fähigkeit, Schwachstellen zeitnah aufzufinden, zu priorisieren und zu beseitigen, ermöglicht es Unternehmen, ihre IT-Systeme kontinuierlich sicherer zu machen und die Angriffsfläche zu reduzieren. Das ist ein laufender Prozess, der nie abgeschlossen sein darf. Für Organisationen, die unter die KRITIS fallen, ist Vulnerability Management Pflicht.

Über Greenbone

Greenbone Networks wurde 2008 von Netzwerksicherheits- und Open-Source-Experten gegründet. Hauptsitz des international agierenden Privatunternehmens ist Osnabrück. Die Greenbone Security Manager (GSM) basieren auf Open Source Software. Sie analysieren IT-Netzwerke auf Schwachstellen und liefern Sicherheitsberichte sowie Hinweise zur Behebung, bevor Angreifer die Sicherheitslücken ausnutzen können. Bestandteil der Lösungen ist ein tägliches, automatisches Security Update. Es bündelt Prozeduren zur Erkennung von aktuellen Sicherheitsproblemen und überwacht Desktop-PCs, Server, Anwendungen und intelligente Komponenten wie etwa Router oder VoIP-Geräte. Die Greenbone-Lösung ist inzwischen eine wichtige Sicherheitskomponente in über 30.000 professionellen Installationen und Integrationen quer durch alle Branchen und Unternehmensgrößen. Die Greenbone Vulnerability Management Software wurde bereits mehr als 2,5 Millionen Mal heruntergeladen.

Weitere Informationen unter **greenbone.net**
Folgen Sie uns auf Twitter: **twitter.com/GreenboneNet**