Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung

IT- und Cyber-Sicherheit im Finanzsektor

Zunehmende Cyber-Kriminalität verlangt nach innovativen Lösungen

Finanzinstitute in Schwellen- und Entwicklungsländern sind zunehmend Ziel von Cyber-Attacken

Digitale Raubüberfälle durch immer komplexere Cyber-Attacken sind weltweit Realität im digitalen Finanzsektor. Besonders bedroht sind kleine und mittlere Finanzinstitute in Schwellen- und Entwicklungsländern, die zu wenig in die erforderliche Absicherung ihrer Systeme investieren.

Cyber-Attacke auf die *Bangladesh Bank*

Im Jahr 2016 versuchten Hacker 951 Millionen US-Dollar von der Zentralbank in Bangladesch zu erbeuten. Letztendlich konnten sie über das Eindringen in das interne IT-System und die Manipulation von Überweisungen 81 Millionen US-Dollar entwenden.

Zudem steigen – durch die rasant zunehmende Nutzung digitaler Finanzprodukte und virtueller Interaktion – Cyber-Bedrohungen für Anbieter auch außerhalb ihrer eigenen Netzwerke aufgrund unsicherer mobiler Kundengeräte. Vor allem in Entwicklungsländern, wo oft mehr Menschen eine *Mobile Wallet* als ein klassisches Bankkonto besitzen, ist das problematisch. Eine Studie der *University of Florida* zeigte, dass die meisten *Mobile Wallet* Applikationen Schwachstellen bei der Daten- und Systemsicherheit aufweisen – nur eine der 46 getesteten Applikationen wurde als sicher eingestuft.

All dies stellt Regulierungs- und Aufsichtsbehörden in den Partnerländern der deutschen Entwicklungszusammenarbeit vor eine Reihe von Herausforderungen. Neben schwachen Cyber-Abwehrsystemen der Finanzinstitute sowie begrenzten personellen und finanziellen Kapazitäten zum Aufbau dieser Systeme zählen hierzu auch Hindernisse bei der Strafverfolgung. Darüber hinaus ergeben sich komplexe Fragen in Bezug auf Gerichtsbarkeit, Zuständigkeiten, grenzüberschreitender Zusammenarbeit und Konsistenz von Gesetzen zu Cyber-Kriminalität zwischen den verschiedenen Ländern.

Die internationale Gemeinschaft reagiert – aber noch zaghaft

Laut der *International Organisation of Securities Commissions* (IOSCO) stellt die Bedrohung der Cyber-Sicherheit ein Risiko für die Integrität, Effizienz und Solidität der globalen Finanzmärkte dar. Im Jahr 2016 haben die G7-Staaten die weitreichenden Auswirkungen der häufiger und komplexer werdenden Cyber-Angriffe auf Finanzinstitute adressiert und die *Cyber Expert Group* (CEG) gegründet, die Cyber-Risiken für den Finanzsektor identifiziert sowie Handlungsansätze erarbeitet. In 2017 stimmten die G20 Finanzminister und Zentralbankchefs überein, dass Cyber-Attacken eine permanente Bedrohung für das gesamte Finanzsystem darstellen. Fortlaufende Maßnahmen seien erforderlich, um die Cyber-Resilienz und Cyber-Sicherheit des Finanzsektors zu gewährleisten. Dieser Aspekt ist auch Teil der Digitalisierungsstrategie des Bundesministeriums für wirtschaftliche Zusammenarbeit und Entwicklung, das bei der entwicklungspolitischen Unterstützung von IT-Lösungen darauf achtet, dass diese anforderungsgerecht abgesichert sind und Personal in den sicheren Anwendungen ausgebildet ist.

Engagement der deutschen Entwicklungszusammenarbeit

Die deutsche EZ arbeitet mit Zentralbanken und Aufsichtsbehörden, Banken- und Versicherungsverbänden sowie Partnern in der IT-Branche zusammen, um den Aufbau von Kapazitäten in den Bereichen IT-Sicherheit und Cyber-Resilienz zu unterstützen. Dabei greift die deutsche EZ auf Erfahrungen des deutschen Regulierungs- und Aufsichtsgesetzgebungsrahmens zu Cyber-Sicherheit im Finanzsektor zurück und transferiert erforderliches Wissen. Dies umfasst z. B. den Dialog zwischen dem öffentlichen und dem privaten Sektor sowie Maßnahmen der Privatwirtschaft, insbesondere der Finanzinstitutionen, zur Verbesserung ihrer eigenen Cyber-Resilienz.

Daten- und IT-Sicherheit für eine Gesundheitsrisikomanagement App in Indien und Pakistan

In einer Strategische Allianz mit der Allianz SE, dem *InsurTech* BIMA und dem *Startup Medicount* wurde eine App zum Gesundheitsrisikomanagement entwickelt, über die eine große Menge von sensiblen Daten gesammelt und genutzt wird. Simulierte Hack-Angriffe auf die App helfen dabei, Sicherheitslücken zu erkennen und zu behoben. Um den Schutz persönlicher Daten zu gewährleisten, werden unter anderem Standards gemäß der EU Datenschutz-Grundverordnung (DSGVO) inkl. Datenschutzhinweise für Kunden und Kundinnen integriert.

Die deutsche EZ achtet auch auf die Einhaltung internationaler Standards der Cyber-Sicherheit. Hier findet insbesondere auch eine eigens für Vorhaben der finanziellen Zusammenarbeit (FZ) entwickelte Checkliste für Cyber-Sicherheit Anwendung. Diese ermöglicht eine erste Risikoabschätzung der FZ-Projektpartner in den Bereichen Informationssicherheit, Datenschutz und Cyber-Sicherheit. Darauf basierend wird entschieden, ob eine detaillierte Cyber-Sicherheitsanalyse notwendig ist oder nicht.

Empfehlungen für Akteure der internationalen Entwicklungszusammenarbeit

- Sensibilisierung von Finanzinstituten, Versicherungen, Führungskräften und Aufsichtsbehörden für die Notwendigkeit von Cyber-Sicherheitsstrategien.
- Unterstützung der Koordinierung zwischen Finanzsektorbehörden und Finanzinstituten, einschließlich Versicherern und anderen Institutionen, die sich mit Cyber-Risiken und Cyber-Sicherheit befassen.
- Konzipierung und Förderung von Aus- und Weiterbildungsprogrammen für technische Spezialisten und Spezialistinnen, qualifizierte Analysten und Analystinnen sowie die Entwicklung von Cyber-Resilienz Trainings für Regulierungsbehörden und Finanzinstitute.
- Unterstützung von Aufsichtsbehörden bei der Beratung von Finanzinstituten, Verbrauchern und Verbraucherinnen.
- Unterstützung des Aufbaus von Netzwerken und Kapazitäten, um die IT-Systeme von Finanzinstituten sicherer zu gestalten, z. B. durch den Bau von technischen Firewalls.
- Förderung der Aufklärung und Sensibilisierung der Internetnutzer und -nutzerinnen in den Partnerländern für Cyber-Kriminalität.

Herausgeber
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)
Referat 110

Stand
11/2020

Kontakt
RL110@bmz.bund.de
www.bmz.de

Postanschrift der BMZ Dienstsitze
BMZ Berlin
Stresemannstraße 94
10963 Berlin
T +49 (0)30 18 535-0

BMZ Bonn
Dahlmannstraße 4
53113 Bonn
T +49 (0)228 99 535-0

Redaktion
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Sitz der Gesellschaft
Bonn und Eschborn

Abteilung Wirtschaft, Soziales, Digitalisierung
Sektorvorhaben Finanzsystementwicklung

Kontakt: sv.fse@giz.de
www.giz.de