FinanzRESILIENZ in Österreich stärken

Technologischen Wandel und geopolitische Spannungen meistern!

VORWORT

Michael Brönner
Geschäftsführer Mastercard Österreich

Simone Wießmeyer
Director & Head of Public Policy DACH, Mastercard

In einer Zeit des beispiellosen technologischen Wandels und zunehmender geopolitischer Spannungen steht die globale Finanzstabilität vor neuen und komplexen Herausforderungen. Mastercard, als eines der globalen Unternehmen im digitalen Zahlungsverkehr, nimmt eine entscheidende Rolle in dieser sich nachhaltig verändernden Lebensrealität ein.

Unsere Wirtschaft, und damit auch das Finanzwesen, stehen heute vor beispiellosen Herausforderungen, die über klassische Risiken hinausgehen. Globale Unsicherheiten, rasante technologische Fortschritte, eine noch nie dagewesenes Maß an Konnektivität sowie exponentiell wachsende Datenmengen führen zu wachsenden Bedrohungen durch Cyberkriminalität wie beispielsweise Ransomware-Attacken, durch Künstliche Intelligenz (KI) gesteuerte Cyberkriminalität, betrügerische Social Engineering-Angriffe oder neue Möglichkeiten für Geldwäsche im Crypto-Umfeld sind längst Realität.

In dieser komplexen Landschaft wird **Resilienz** – die Fähigkeit, Krisen zu bewältigen und sich schnell von Schocks zu erholen – zur Schlüsselkompetenz, um langfristige Stabilität und Sicherheit zu gewährleisten. Ein zentraler Aspekt ist die zunehmende Bedeutung der **Cyberresilienz**. Neue Technologien beeinflussen die Art und Weise, wie wir leben und arbeiten. Diese Fortschritte haben jedoch auch ein **erhöhtes Risiko von Cyberkriminalität** und damit einhergehend einen sich schnell entwickelnden Bedarf für effektive Cybersicherheit geschaffen.

Natürlich sind wir selbst, als Privatpersonen aber auch als Unternehmen, fasziniert von den neuen Möglichkeiten und dem Fortschritt, den neuen Technologien für den Zahlungsverkehr und unser tägliches Bezahlverhalten in Bezug auf Sicherheit, Einfachheit und Geschwindigkeit leisten können. Aber wie immer gilt – es gibt zwei Seiten der Medaille: **Auch die „Bad Guys" haben Zugang zu diesen Technologien und nutzen sie als Waffe, um Geld, Daten und Wissen zu erbeuten.**

- Verschiedene Studien der jüngeren Vergangenheit gehen davon aus, dass mittlerweile die Hälfte des gesamten Internetverkehrs von Bots ausgeht, die Schnittstellen und Websites angreifen, was durch leistungsfähigere Rechen- und Verarbeitungsfunktionen überhaupt erst möglich wird.
- Betrüger nutzen neue Technologien, wie beispielsweise KI, auf immer innovativere und raffiniertere Weise, um Verbraucher:innen auszutricksen, und das Problem wächst: Die weltweiten Kosten und entgangenen Einnahmen durch Cyberangriffe werden im Jahr 2025 schätzungsweise 10,5 Billionen US-Dollar betragen.[1]
- Die Betrüger wissen, dass der Endnutzer heute das schwächste Glied in der Abwehrkette von Cyberbedrohungen ist – das ist ein Problem für Verbraucher:innen, Unternehmen sowie staatliche Institutionen.

- Laut der von KPMG gemeinsam mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum Sicheres Österreich durchgeführten Studie „Cybersecurity in Österreich" stieg die Anzahl der Angriffe im Jahr 2023 um 201 Prozent. Fast die Hälfte der Befragten Unternehmen erlitt Schäden von bis zu 100.000 Euro.

„Seit 2018 haben wir weltweit sieben Milliarden US-Dollar in Cybersecurity investiert – über eine Milliarde pro Jahr. Mit dem Mastercard Europan Cyber Resilience Centre haben wir zusätzlich einen Ort geschaffen, an dem wir externe Expert:innen einladen, um den gemeinsamen Informationsaustausch zu intensivieren und die Resilienz des Finanzsystems zu stärken."

Michael Brönner, Geschäftsführer Mastercard Österreich

Unser Anspruch bei Mastercard ist es, den Cyberkriminellen immer zwei Schritte voraus sein.

Um dies zu erreichen, werden wir weiterhin Trends und neue Betrugsszenarien beobachten und unsere weltweit führende Technologie nutzen, um neue Lösungen zu entwickeln, die unser digitales Ökosystem – und das unserer Partner – schützen.

Dabei wollen wir beispielsweise:

- Stets neuste Technologie, wie aktuell zum Beispiel KI-Modelle, einsetzen, um den Schutz der Verbraucher:innen und des gesamten Zahlungsnetzwerks kontinuierlich zu verbessern. Unsere Erfahrungswerte beruhen auf 143 Mrd. Zahlungstransaktionen, die wir pro Jahr bearbeiten. Anhand dieser Daten lernt unser Algorithmus und kann in nahezu allen Fällen vorhersagen, ob ein Transfer legitim ist oder nicht. **Allein im letzten Jahr wurden Transaktionen im Wert von 20 Mrd. US-Dollar als betrügerisch eingestuft und von uns gestoppt.**

- Die Zusammenarbeit mit unserem globalen Partnernetz weiter ausbauen. Das in diesem Jahr eröffnete **European Cyber Resilience Centre (ECRC)** an unserem europäischen Hauptsitz in Waterloo, Belgien, ist ein wichtiger neuer Bestandteil dieser Strategie. Das ECRC unterstützt Cybersicherheits- und Strafverfolgungsbehörden sowie Branchenverbände in ganz Europa.

Das hochmoderne **European Cyber Resilience Centre (ECRC)** bringt Vertreter:innen aus dem privaten und öffentlichen Sektor an einen Tisch, um gemeinsam Abwehrmaßnahmen gegen Cyberbedrohungen zu verbessern und Reaktionszeiten auf Cyber-Angriffe zu optimieren. Das ECRC besteht aus einem „Fusion Center", an dem Mastercards Incident Response Team ansässig ist, sowie einem Labor für digitale Forensik. Dort arbeiten Vertreter:innen von mehr als 20 Teams zusammen.

Als einzelne Organisation können wir viel erreichen, jedoch ist unser Hebel als Teil eines globalen Netzwerks viel größer.

Wir sind der festen Überzeugung, dass eine eng vernetzte digitale Wirtschaft für die Widerstandsfähigkeit der Welt – indem sie die Bürgerinnen und Bürger miteinander verbindet und den Handel aufrechterhält – ein wichtiger Faktor für Österreich und letztlich auch Europas exportstarke Nationen ist. Genau diese globale Dimension der Vernetzung ist wichtig, wenn es um die Stärkung der Cyberresilienz in Österreich geht. Es ist daher von entscheidender Bedeutung, die internationale Zusammenarbeit in Governance-Fragen sowie die Etablierung globaler Standards und die Förderung öffentlich-privater Partnerschaften zu intensivieren. Auch die Politik sollte gezielt Initiativen zur Bekämpfung der Cyberkriminalität unterstützen. Es braucht innovative regulatorische Rahmenbedingungen, die die Nutzung neuer Technologien wie KI und Biometrie ermöglicht und erleichtert, um so Betrugsbekämpfung zu verbessern.

Die aktuellen Entwicklungen und damit verbundenen Initiativen unterstreichen die **Notwendigkeit einer engen Zusammenarbeit zwischen privaten und öffentlichen Akteuren**, um Cyberkriminalität effektiv zu bekämpfen.

Dieses Whitepaper beleuchtet die vielfältigen Aspekte der Finanzresilienz und zeigt, wie wichtig Maßnahmen auf unterschiedlichen Ebenen sind – von der Finanzbildung über technologische Innovationen bis hin zu politischen Initiativen und zukunftsfähigen regulatorischen Rahmenbedingungen.

Für eine stärkere **Resilienz** spielt auch die **finanzielle Bildung** eine wesentliche Rolle. Sie bildet das Fundament, um Menschen und Gesellschaften besser auf finanzielle Herausforderungen vorzubereiten, Bedrohungen im Cyberraum zu erkennen und in Krisenzeiten handlungsfähig zu bleiben. Gleichzeitig sind **politische Maßnahmen** von zentraler Bedeutung. Die Österreichische **Sicherheitsstrategie (ÖSS)** betont die Wichtigkeit einer robusten Finanzpolitik und Aufsicht, die eng mit anderen Bereichen verknüpft ist. Initiativen wie der **Digital Operational Resilience Act (DORA)** der EU zielen darauf ab, das Finanzsystem gegen Cyberrisiken abzusichern und gleichzeitig Innovationen zu fördern.

„Die zunehmenden globalen Unsicherheiten verlangen nach einem klaren politischen Rahmen, der Finanzresilienz unterstützt. Durch enge Zusammenarbeit zwischen Regierungen und dem privaten Sektor können wir sicherstellen, dass wir nicht nur auf aktuelle Bedrohungen vorbereitet sind, sondern auch langfristig die Stabilität des Ökosystems sichern."

Simone Wießmeyer, Director Public Policy, Head of DACH Region, Mastercard

Ganz entscheidend für die Steigerung der Widerstandsfähigkeit von Unternehmen gegen Cyberrisiken sind technologische Innovationen, um besser gegenüber neuen Angriffszenarien (z.B. durch Ransomware) aufgestellt zu sein. Auch dieser Aspekt und die rechtlichen Möglichkeiten werden im vorliegenden

Whitepaper beleuchtet. Die enge Verbindung zwischen **Finanzresilienz und Innovation** wird deutlich: Eine starke finanzielle Grundlage ist die Voraussetzung für technologische Fortschritte, die wiederum die Resilienz des Finanzsystems stärken.

Dieses Whitepaper soll Impulse geben und konkrete Ansätze aufzeigen, wie Österreich seine FinanzRESILIENZ weiter ausbauen kann.

Das enge Zusammenspiel von Bildung, Technologie, politischen Rahmenbedingungen und internationaler Kooperation ist unerlässlich, um ein widerstandsfähiges und zukunftssicheres Ökosystem für das Finanzwesen und die Wirtschaft zu schaffen.

Wir danken allen Beteiligten für ihre wertvollen Beiträge und wünschen eine inspirierende Lektüre.

INHALTSVERZEICHNIS

1. Wie gelingt Finanzmarktstabilität?

MMag. Martin Sprengseis-Kogler
Managing Partner &
Board of Advisors, bluesource –
mobile solutions gmbh
Initiator, P19

„Finanzresilienz" auf Basis von Finanzbildung

Finanzresilienz durch Financial Literacy: Eine entscheidende Verbindung

In einer von Unsicherheiten geprägten Welt wird die Fähigkeit, finanzielle Schocks zu bewältigen und Stabilität zu wahren, immer wichtiger. Diese Finanzresilienz beschreibt die Kapazität, unvorhergesehene finanzielle Belastungen wie Einkommensverluste oder wirtschaftliche Krisen zu absorbieren und dennoch finanzielle Stabilität zu bewahren. Finanzresilienz ist entscheidend für langfristige Sicherheit und Wohlstand, da sie soziale Ungleichheiten verringert und die allgemeine wirtschaftliche Stabilität fördert.

Das Fundament der Finanzresilienz ist „Financial Literacy" – also finanzielle Bildung. Sie vermittelt das Wissen und die Fähigkeiten, um fundierte finanzielle Entscheidungen zu treffen, Risiken zu minimieren und langfristige Sicherheit zu erreichen. Ohne ausreichende Financial Literacy sind Menschen anfälliger für finanzielle Schocks und haben größere Schwierigkeiten, sich davon zu erholen.

Verbindung zwischen Financial Literacy und Finanzresilienz

Financial Literacy bildet die Grundlage für Finanzresilienz, indem sie Menschen dazu befähigt, grundlegende Finanzkonzepte wie Budgetierung, Sparen und Schuldenmanagement zu verstehen und anzuwenden. Diese Fähigkeiten sind unerlässlich, um eine stabile finanzielle Basis zu schaffen, die auch in wirtschaftlich unsicheren Zeiten Bestand hat.

Die zunehmende Digitalisierung der Finanzwelt ist ein wesentlicher Aspekt moderner Finanzbildung. Die Smartphone-Nutzung ist auf rund vier Stunden pro Tag gestiegen, was die Art und Weise, wie Menschen Finanztransaktionen durchführen und sich über Finanzen informieren, grundlegend verändert hat. Mobile Finanz-Apps und digitale Zahlungsdienste haben den Zugang zu Finanzdienstleistungen erleichtert, erfordern jedoch ein neues Verständnis von Sicherheit und Risiko.

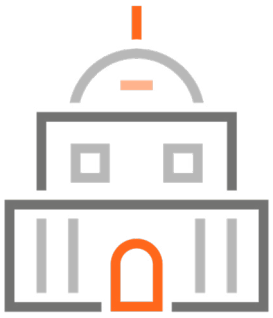
Besonders wichtig ist es, alle Altersgruppen auf diese geänderte Nutzung des Zahlungsverkehrs hinzuweisen und entsprechende Bildungsmaßnahmen anzubieten. Während jüngere Generationen mit Smartphones vertraut sind, fehlt ihnen oft das Bewusstsein für die langfristigen Auswirkungen ihres Finanzverhaltens. Ältere Generationen stehen vor der Herausforderung, sich an neue Technologien anzupassen und traditionelle Finanzpraktiken weiterhin zu verstehen.

In Österreich wurden 2021 im Rahmen der **Nationalen Finanzbildungsstrategie** verschiedene Maßnahmen wie Seminare für Lehrkräfte und Wettbewerbe zur Förderung der Finanzbildung eingeführt. Eine langfristige Bewertung dieser **Maßnahmen** (siehe Excel-Dokument) steht jedoch noch aus. Angesichts steigender Cyberkriminalität zeigt sich, dass Präventionsmaßnahmen und der Anstieg von Betrugsfällen im digitalen Zahlungsverkehr auseinanderklaffen – ein Indiz für unzureichende Finanzbildung in der Bevölkerung. Ein großer Bildungsauftrag liegt vor uns, um die Digitalisierung im Zahlungsverkehr zu begleiten und die Vorteile optimal zu nutzen.

Herausforderungen in der Finanzkompetenz

Trotz der großen Bedeutung von Financial Literacy gibt es erhebliche Herausforderungen. Finanzbildung ist oft nicht systematisch in den Lehrplänen von Schulen verankert, was zu erheblichen Bildungslücken führt. Diese Lücken können sich im Erwachsenenalter vergrößern, wenn keine weiteren Weiterbildungsangebote bestehen.

Die heutige Finanzlandschaft ist komplexer als je zuvor. Neue Finanzprodukte wie Kryptowährungen oder komplizierte Anlagemodelle können selbst für finanzgebildete Menschen schwer verständlich sein. Diese Komplexität erschwert fundierte Entscheidungen und erhöht das Risiko, in ungeeignete oder riskante Finanzprodukte zu investieren.



Verschiedene Bevölkerungsgruppen stehen vor unterschiedlichen Herausforderungen. Jugendliche und junge Erwachsene haben oft wenig praktische Erfahrung im Umgang mit Geld und geraten leicht in Schuldenfallen. Geringverdiener haben Schwierigkeiten, Zugang zu Finanzprodukten zu erhalten, die ihnen beim Vermögensaufbau helfen könnten. Senioren, die nicht mit digitalen Technologien vertraut sind, sind anfällig für Betrug und haben oft Schwierigkeiten, sich in der digitalen Finanzwelt zurechtzufinden.

Eine mögliche Lösung liegt in grenzüberschreitender Aufklärung und technologischen Lösungen, die jedoch internationale Zusammenarbeit erfordern. Ein positives Beispiel für nationale Zusammenarbeit ist die **Kooperation zwischen dem Clearinghaus PSA (Payment Services Austria) und dem Bundeskriminalamt**.

Ein weiteres Hindernis ist die fehlende Sensibilisierung für digitale Finanztechnologien. Obwohl Smartphones und mobile Finanz-Apps weit verbreitet sind, fehlt vielen Menschen das Verständnis für die sichere Nutzung dieser Tools. Besonders ältere Menschen könnten den Anschluss verlieren und damit ihre Finanzresilienz gefährden.

Kulturelle und soziale Barrieren beeinträchtigen ebenfalls die finanzielle Bildung. In einigen Gemeinschaften ist es tabu, über Geld zu sprechen, was der Zugang zu wichtigen Informationen erschwert wird. Diese Barrieren verstärken bestehende Ungleichheiten und erschweren es den Betroffenen, ihre finanzielle Situation zu verbessern.

Schlussfolgerung:
Die Finanzresilienz muss nachhaltig gestärkt werden.

Um die Finanzresilienz in der breiten Bevölkerung zu stärken, ist es unerlässlich, die Financial Literacy systematisch zu fördern und auf die Bedürfnisse verschiedener Bevölkerungsgruppen einzugehen. Bildungsinitiativen müssen sowohl traditionelle Finanzkompetenzen als auch digitale Finanztechnologien abdecken.

Folgende Maßnahmen sind zusammengefasst notwendig:

1. **Integration von Finanzbildung in Schulen:**
   Finanzkompetenz in Lehrplänen verankern.
2. **Lebenslanges Lernen fördern:**
   Weiterbildungsmöglichkeiten für Erwachsene bereitstellen.
3. **Zugang zu digitalen Finanztools erleichtern:**
   Aufklärung über sichere Nutzung von Finanz-Apps.
4. **Zielgruppenspezifische Programme:**
   Spezielle Bildungsinitiativen für Jugendliche, Geringverdiener und Senioren entwickeln.
5. **Öffentliche und private Partnerschaften:**
   Kooperationen zur Förderung umfassender Finanzbildungsprogramme.
6. **Kulturelle Barrieren abbauen:**
   Förderung offener Gespräche über Finanzen.
7. **Einfache Finanzprodukte:**
   Transparente und verständliche Finanzprodukte bereitstellen.

Europa hat die Chance, durch diese Maßnahmen zum globalen Vorreiter in der Finanzbildung zu werden und als „Leuchtturm" für andere Regionen zu dienen.

Dr. Ben-Benedict Hruby
LL.M., Abteilungsleiter,
Bundesministerium für Finanzen
Sektion III – Wirtschaftspolitik und Finanzmärkte, Abteilung III/C/10 – Kapitalmarktrecht und FinTech

Politische Maßnahmen für ein resilientes Finanzsystem

Wir befinden uns in einem zunehmend vernetzten und digitalisierten Zeitalter, welches mit entsprechend höheren Cyberrisiken einhergeht. Auch die Widerstandsfähigkeit des Finanzsystems wird durch ständig neue Risiken, beispielsweise aufgrund des Einsatzes künstlicher Intelligenz, gefordert. Insbesondere in einem so systemrelevanten Sektor wie dem Finanzsektor sind Investitionen in und Maßnahmen zum Schutz vor Cyberrisiken von oberster Priorität. Die Steigerung von Cybersicherheit trägt auch maßgeblich zum Wachstum und Erfolg von Unternehmen bei und ist Voraussetzung für einen sicheren und attraktiven Wirtschaftsstandort.

Die Bewältigung der beschriebenen Herausforderungen erfordert die Zusammenarbeit verschiedener staatlicher und privater Akteure und wirft die Frage auf, welche politischen Maßnahmen notwendig sind, um sich an die veränderte technologische Realität anzupassen und das Ziel eines resilienten Finanzsystems zu erreichen.

Status quo - Bisherige politische Maßnahmen

Die EU erkannte frühzeitig, dass ein Handeln ihrerseits zur Bewältigung der Herausforderungen im Zusammenhang mit Cybersicherheit nötig ist. Bereits 2016 trat mit der NIS 1 Richtlinie eine Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen der EU in Kraft und wurde in Österreich im Netz- und Informationssystemsicherheitsgesetz, welches im Dezember 2018 in Kraft trat, umgesetzt.

In Österreich wurde außerdem mit der Österreichischen Strategie für Cybersicherheit 2021 (ÖSCS 2021) ein umfassendes Konzept um Schutz des Cyberraums und der Menschen im virtuellen Raum beschlossen, welches die Grundlage der gesamtstaatlichen Zusammenarbeit in diesem Bereich bilden soll und ein Bekenntnis Österreichs zu einem Beitrag zur Cybersicherheit der EU enthält. In der ÖSCS 2021 identifizierte Herausforderungen umfassen unter anderem Bedrohungen durch die falsche Nutzung von IT, neue Technologien und durch die zunehmende Abhängigkeit von IT sowie den Mangel an Fachkräften in diesem Bereich. 2024 wurde zur ÖSCS 2021 ein Maßnahmenkatalog inklusive Fortschrittsmessung veröffentlicht, welcher eine Fülle an Maßnahmen – vom Ausbau nationaler Koordinierungszentren bis zur Bildung im Bereich Cybersicherheit – enthält.

Aktuelle Maßnahmen – DORA und NIS 2

Die letzte große Aktualisierung des Politikrahmens zur Cyberbedrohung, durch welche eine Anpassung der EU-Cybersicherheitsstrategie an die digitale Dekade vorgenommen werden soll, umfasst unter anderem eine Überarbeitung der NIS-Richtlinie (NIS 2), sowie eine Richtlinie zur Widerstandsfähigkeit kritischer

Einrichtungen und einer Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA, Digital Operational Resilience Act). Da es sich bei der NIS 2 um eine Richtlinie handelt, ist sie von den Mitgliedsstaaten der EU bis zum 17. Oktober 2024 noch in nationales Recht umzusetzen. Bei der DORA handelt es sich hingegen um eine Verordnung, welche nicht in nationales Recht umgesetzt werden muss, sondern für betroffene Unternehmen ab dem 17. Jänner 2025 unmittelbar anwendbar ist.

Die DORA ist auf eine Vielzahl von Finanzunternehmen, beispielsweise Kreditinstitute, Wertpapierfirmen, Versicherungsunternehmen und Anbieter von Krypto-Dienstleistungen, anwendbar. Unternehmen im Bereich des Bankwesens und Finanzmarktinfrastrukturen fallen zwar grundsätzlich auch unter die NIS 2-Richtlinie, speziellere Bestimmungen der DORA gehen den Bestimmungen der NIS 2 Richtlinie jedoch vor. DORA sieht in folgenden Bereichen Regelungen für Finanzunternehmen vor: Risikomanagement im Bereich Informations- und Kommunikationstechnologien (IKT), verpflichtende Meldung schwerwiegender IKT-bezogener Vorfälle an Behörden sowie freiwillige Meldung erheblicher Cyberbedrohungen, Informationsaustausch, Durchführung von Tests der digitalen Resilienz (inklusive threat-led penetration testing für gewisse Unternehmen) und Risiken durch die Nutzung von IKT-Drittdienstleistern (wie beispielsweise Cloud-Dienstleistern). Für kritische Drittdienstleistungen soll darüber hinaus ein neuer europäischer Überwachungsrahmen geschaffen werden. Bei der Anwendung der DORA ist der Grundsatz der Verhältnismäßigkeit zu beachten und demnach der Größe, dem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität der Dienstleistungen, Tätigkeiten und Geschäfte eines Finanzunternehmens Rechnung zu tragen.

Ausblick und Fazit

In Österreich wurde das DORA-Vollzugsgesetz, welches erforderliche nationale Begleitmaßnahmen zur DORA schaffen soll, im Juli 2024 vom Parlament verabschiedet. Durch dieses Vollzugsgesetz wird beispielsweise eine Klarstellung zur Zuständigkeit der Finanzmarktaufsichtsbehörde (FMA) getroffen und es werden Strafbestimmungen für natürliche und juristische Personen vorgesehen.

Durch die Fülle der beschriebenen Maßnahmen zur Herstellung eines einheitlichen, hohen Cybersicherheitsniveaus ist Österreich auf die veränderte technologische Realität gut vorbereitet und auf dem Weg zur Erreichung eines resilienten Finanzsystems. Dennoch wird auch zukünftig eine Zusammenarbeit staatlicher und privater Akteure sowie eine laufende Anpassung der Maßnahmen zur Bewältigung der Herausforderungen notwendig sein.

2. Innovation und Technologie beeinflussen Finanzresilienz?

Maria Kirschner
Vice President, General Manager der Kyndryl Alps-Region

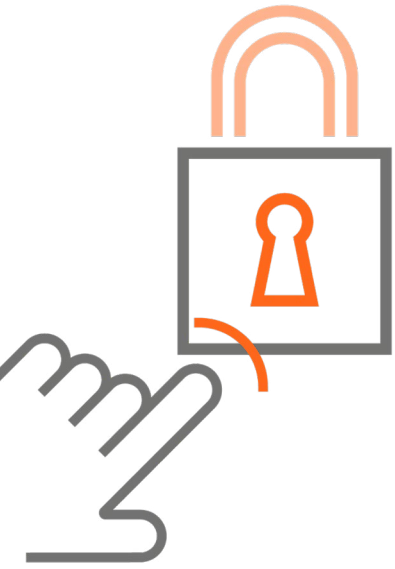
Wie Cybersecurity-Innovationen und das richtige Mindset zum Schutz und zur Wiederherstellung des Betriebs von Finanzdienstleistungen beitragen können

Laut dem EU-Länderbericht zur digitalen Dekade vom Juli 2024 meldeten 3,4% der österreichischen Unternehmen IKT-Ausfälle aufgrund von Ransomware oder Denial-of-Service-Angriffen. Nur ungefähr 27% der österreichischen Unternehmen gaben an, gegen Cyberangriffe versichert zu sein, während 92,5% der heimischen Betriebe IKT-Sicherheitsmaßnahmen zum Einsatz bringen. Statistiken bestätigen die Tatsache, dass es nicht eine Frage ist, „ob" ein Cyberangriff stattfinden wird, sondern „wann". Aus diesem Grund müssen Unternehmen proaktive Maßnahmen ergreifen, um potenzielle Cyber-Angriffe zu erkennen, sich gegen sie zu wehren, sobald diese erkannt werden, und – was am entscheidendsten ist – sich von Störungen mit minimalen Auswirkungen auf den laufenden Geschäftsbetrieb rasch wieder zu erholen.

Ein Großteil der Unternehmen setzt auf den Einsatz umfangreicher Technologie, um das Problem zu lösen, aber das ist nicht die ganze Antwort. Eine ganzheitlichere Lösung besteht darin, zu wissen, welche Technologien vorhanden sind, indem man ein gutes Inventarsystem einsetzt und dafür sorgt, dass diese Systeme gepatcht, gegen Angriffe geschützt, kontinuierlich überwacht und für eine schnelle Wiederherstellung geeignet sind. In anderen Worten: Unternehmen müssen sich eine Cyber-Resilienz-Mentalität zu eigen machen und eine Arbeitsweise etablieren, welche die Unvermeidbarkeit von Cyber-Störungen akzeptiert und sich auf Resilienz fokussiert.

Diese Cyber-Resilienz-Mentalität ist besonders in einem technologischen Kontext wichtig, in dem KI in den nächsten Jahren wahrscheinlich das Volumen und die Auswirkungen von Cyberangriffen erhöhen wird. So erhöht generative KI beispielsweise das Risiko erfolgreicher Manipulationen, indem sie äußerst realistische und ausgefeilte Phishing-Angriffe mit Malware ermöglicht, die herkömmliche Kontrollmechanismen erfolgreicher umgehen können. Unternehmen sind daher gut beraten, sich mit KI-gestützter Abwehr auszustatten, die stärker ist als KI-gestützte Cyberbedrohungen.

Wir sehen, dass KI und generative KI eine immer wichtigere Rolle für Unternehmen dahingehend spielen, Bedrohungen zu erkennen, sich entsprechend zu schützen und den Betriebszustand bei minimaler Unterbrechung wiederherzustellen. Hierfür gibt es eine Vielzahl von Möglichkeiten:



- **Erkennung und Prävention von Bedrohungen:** KI-gestützte Sicherheitssysteme können den Netzwerkverkehr kontinuierlich überwachen, Anomalien erkennen und potenzielle Sicherheitsrisiken in Echtzeit identifizieren.
- **Risikoanalyse und -management:** KI-gestützte Tools zur Bewertung von Risiken können umfangreiche Datenmengen analysieren, um potenzielle Schwachstellen zu identifizieren und ihre Auswirkungen auf die Einhaltung von Cybersecurity-Vorschriften zu bewerten. Diese Tools können Gefahren nach Schweregrad und Wahrscheinlichkeit priorisieren, um dabei zu helfen, Probleme zu stoppen, bevor sie entstehen, sowie wichtige Entscheidungen über die Ressourcenverteilung zu treffen.
- **Datenschutz und Einhaltung der Privatsphäre:** KI-Technologien wie maschinelles Lernen und natürliche Sprachverarbeitung können dazu beitragen, die Bemühungen zum Datenschutz und zur Einhaltung der Privatsphäre zu verbessern. Sie unterstützen bei der Klassifizierung sensibler Daten, der Durchführung von Zugriffskontrollen, der Kontrolle der Datennutzung im Hinblick auf die Einhaltung von Datenschutzbestimmungen und der Erkennung von Datenschutzverletzungen.
- **Reaktion auf Vorfälle und Behebung:** KI ermöglicht es, die Erkennung, Analyse und Behebung von Sicherheitsvorfällen zu automatisieren. KI kann ebenfalls dazu beitragen, Reaktionszeiten zu verkürzen und so die Auswirkungen von Sicherheitsverletzungen zu minimieren.

Für den Finanzdienstleistungssektor sind diese neuen Kompetenzen insbesondere im Zusammenhang mit dem Digital Operational Resilience Act (DORA) von Bedeutung, der im Jänner 2025 in Kraft treten wird. Zusammen mit ähnlichen neuen und künftigen Regulierungen in der gesamten digitalen Wirtschaft bietet DORA einen kodifizierten und standardisierten Ansatz, der dazu beiträgt, dass Finanzunternehmen in der EU, diejenigen, die weltweit mit ihnen zusammenarbeiten, sowie ihre IT-Dienstleister einen klaren Weg zu effektiver Cyber-Resilienz finden.

Die Umsetzung von Richtlinien kann eine Herausforderung darstellen. Wenn es Unternehmen an qualifizierten Fachkräften mangelt, um unternehmenskritische Änderungen zu implementieren, sollten sie mit einem Partner kooperieren, der sowohl geschäftliche als auch technologische Erfahrung hat.

Vermehrt versuchen Länder und Regionen, einheitliche und effektive Maßnahmen zur Gewährleistung der Geschäftskontinuität zu etablieren. So können sich österreichische Unternehmen und ihre kompetenten Partner gemeinsam auf die Herausforderungen der sich ständig wandelnden Bedrohungslage im Bereich Cybersecurity und die komplexe Erfüllung von gesetzlichen Vorschriften vorbereiten.

Dr. Isabell Claus
Managing Director, thinkers GmbH

Finanzresilienz: Die zentrale Grundlage für Innovation

„Man nennt es erst Innovation, wenn es jemanden gibt, der für eine Idee oder Erfindung bereit ist, etwas zu zahlen. Erst wenn Innovation einen Markt findet, gewinnt sie an Wert." So lehren es seit Jahrzehnten die Wirtschaftsuniversitäten. Künstliche Intelligenz ist in dieser Hinsicht eine der größten Innovationen, die die Menschheit je gesehen hat, denn sie bewegt Milliarden von Investor:innen und Kund:innen auf dem globalen Markt.

Wie würde diese Innovation, die unter anderem neue, entscheidende Erkenntnisse in der Medizin und vielen anderen Wissenschaften, die für Leben und Wohlstand herausragende Fortschritte ermöglichen, wachsen, wenn wir keine Finanzresilienz als Grundlage unserer Zeit hätten? Es gäbe viele Fragezeichen und Hürden auch wenn die Innovation an sich noch so groß ist. Es würden sich wesentlich weniger Investor:innen, Kund:innen, Nutzer:innen und wiederum neue Innovator:innen und Weiterentwickler:innen finden, die in kürzester Zeit handlungsbereit sind, quasi über Nacht Investitionen verfügbar machen können und so fest an die neuen und zukünftigen Errungenschaften glauben, dass sie kurzfristig sehr große Ressourcen einsetzen.

Finanzresilienz wird in derartigen Betrachtungen des Öfteren als selbstverständlich gesehen, obwohl sie es nicht ist. Disruptive technologische Innovation hat nicht zuletzt das Potential, vor allem staatliche „Hüter" der Finanzresilienz inhaltlich und in punkto Schnelligkeit zu überholen. Finden disruptive Ansätze in kürzester Zeit viele Anhänger:innen, ist wiederum die Finanzresilienz in Gefahr. Dabei spielen Ländergrenzen wohl keine Rolle mehr – das gilt sowohl für Innovation als auch für Finanzresilienz. Entscheidungen und Geschehnisse finden de facto nicht mehr lokal statt, sondern in einem komplexen Geflecht aus internationalen Stakeholdern. Die Planbarkeit und Übersichtlichkeit dessen ist also nur eingeschränkt möglich. Eine internationale „Prävention" von Krisen ist ebenso komplex und oftmals stehen konträre Interessen dem Ziel im Weg, einheitliche internationale Regeln zu vereinbaren. Die Grenzen von Regulatorik sind also in dieser Hinsicht heute immer noch viel enger als die Grenzen, die technologische Innovation in kürzester Zeit überwindet. Passt das Gefüge zusammen?

Vor diesem Hintergrund müssen immer größere Anstrengungen von sehr vielen Stakeholdern gemacht werden, um Finanzresilienz als Basis für die Widerstandsfähigkeit des Gesamtsystems unserer Zeit, zu erhalten. Wie gehen wir an so eine „Mammutaufgabe", die sowohl für uns als Innovation:innen als auch für die künftigen Generationen von großer Bedeutung ist, heran?

Bis ins letzte Detail ist das realistisch wohl nicht zu beantworten, gewisse Grundsatzfaktoren können jedoch zugerechnet werden: So werden Anstrengungen nur fruchten, wenn sie viele Stakeholder „im Boot" haben, möglichst breitflächig - in jedem Falle grenzüberschreitend - als vereinbarte Regeln und Standards angenommen und gelebt werden sowie ein zielführender Informations- und Datenaustausch gewährleistet ist.

Das „Must have", das diesen Charakteristiken in 2024 hinzugefügt werden sollte, betrifft eine kontinuierlich höhere Schnelligkeit in der Handlungsfähigkeit und Koordination aller Stakeholder. Die „VUCA-Welt" (volatility, uncertainty, complexity, ambiguity) hat in den letzten Jahren allen Menschen eine vorher kaum gekannte Schnelligkeit bei signifikanten Entscheidungen und Handlungen abverlangt. Auch aufgrund der Ausbreitung von Krankheiten und Kriegen ist die „KI-Welle" ein Bereich, in dem keine Zeit für Pausen geblieben ist.

Wird es zukünftig weniger schnell, weniger komplex oder weniger innovativ? Dafür gibt es keinerlei Anzeichen. Daher ist es ratsam, die Charakteristiken unserer Zeit, die allem voran auch die jetzige und zukünftige Finanzresilienz beeinflussen, als einen sich ständig weiterentwickelnden Gestaltungsspielraum zu verstehen, der im Sinne der (unter anderem für Innovation) notwendigen gesamtheitlichen Widerstandsfähigkeit mit zeitgemäßen Methoden auf Basis eines gemeinsamen Zukunftsbildes (das viele Stakeholder mittragen wollen) gestaltet werden sollte. Wichtig sind ist dabei das Zusammenspiel zwischen Menschen und Maschinen.

3. Geopolitische Maßnahmen für funktionierende Finanzresilienz

Dr. Franz Rudorfer
Wirtschaftskammer Österreich, Geschäftsführer der Bundessparte Bank und Versicherung

Philipp Horvath BSc LL.M.
Referent Wirtschaftskammer Österreich, Generalsekretariat (Abteilungen, Bundessparten, Fachorganisationen), Bundessparte Bank und Versicherung

Finanzresilienz in turbulenten Zeiten: Der Weg nach vorne

Die aktuelle geopolitische Lage zeigt uns mehr als eindrücklich, wie rasch sich globale Spannungen und technologische Innovationen auf unser Finanzsystem auswirken können. In einer Zeit, in der Unsicherheit zur neuen Normalität geworden ist, müssen wir den Fokus auf Resilienz legen. Albert Einstein sagte: „In der Mitte von Schwierigkeiten liegen Möglichkeiten." Dieser Gedanke ist heute aktueller denn je, denn die Herausforderungen, vor denen wir stehen, sind zugleich Chancen, unser Finanzsystem noch widerstandsfähiger zu gestalten.

Geopolitische Turbulenzen und technologische Risiken

Die geopolitischen Spannungen der letzten Jahre haben unsere globale Vernetzung auf die Probe gestellt. Handelskonflikte, politische Unsicherheiten und sogar Kriege (leider in der Mehrzahl) beeinflussen die Finanzwelt stärker als je zuvor. Der technologisch beschleunigte Wandel bringt zwar Fortschritte und Möglichkeiten, eröffnet jedoch gleichzeitig auch neue Angriffsflächen für Cyberkriminalität und Betrug. Die KI lernt wöchentlich kontinuierlich dazu: Wer weiß, zu was sie in einigen Jahren im Stande sein wird? Quantum Computer können möglicherweise in wenigen Jahren jede endverschlüsselte Botschaft knacken. Social Engineering und andere Angriffe auf unsere digitale Finanzinfrastruktur nehmen rasant zu. Vor diesem Hintergrund müssen wir uns fragen, ob unsere Systeme digitalen Schwarzer-Schwan-Ereignissen gewachsen sind.

Regulierung und die Illusion der Kontrolle

Der auf Finanzstabilität spezialisierte Ökonom Jon Danielsson hat die „Illusion of Control" treffend beschrieben. Wir neigen dazu, uns in Sicherheit zu wiegen, wenn wir vermeintlich die Kontrolle über komplexe Systeme haben. Dies vermittelt oft das Gefühl, dass ein umfassendes Regelwerk ausreichend ist, um Risiken umfassend zu managen. Um die „Illusion of Control" zu vermeiden, müssen Regulierungsbehörden und Finanzinstitutionen einen Weg finden, der die richtige Balance zwischen Regulierung und Flexibilität sicherstellt. Ein starres Regelwerk allein kann nicht auf unvorhersehbare Ereignisse oder gar komplexe Entwicklungen reagieren. Eine flexible, risikobewusste und proportionale Herangehensweise ist notwendig, um ein resilienteres Finanzsystem zu schaffen. Auch ein effizienter Datenaustausch über potentielle und akute Gefahrenlagen ist essentiell. Der Digital Operational Resilience Act (DORA) bringt harmonisierte Regeln für den gesamten Finanzsektor, um die digitale Resilienz zu stärken. Finanzinstitute haben strenge Sicherheitsstandards einzuhalten, um ihre Systeme und Kunden vor digitalen Bedrohungen zu schützen. Aber wir dürfen

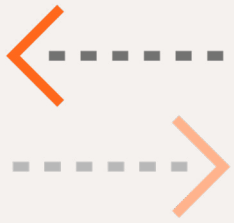
uns nicht ausschließlich darauf verlassen, dass Regulierung allein uns vor den Unwägbarkeiten der modernen Welt schützt, vor allem wenn sie nicht alle Akteure erfasst oder erfassen kann.

Bürokratie: Bremsklotz oder Schutzmechanismus?

Die Balance zwischen Regulierung und Flexibilität ist entscheidend für die Resilienz des Finanzsystems. Zu viel Bürokratie behindert Innovation und schränkt die Anpassungsfähigkeit ein. Ein ausbalancierter Mittelweg, der sowohl Sicherheit als auch Kreativität fördert, muss das Ziel sein. Von diesem Mittelweg haben wir uns in den letzten Jahren jedoch immer weiter entfernt. Bürokratische Hürden abzubauen, während wir gleichzeitig die Sicherheit unserer Finanzinfrastruktur gewährleisten, sollte sowohl unsere als auch vor allem Priorität der Regulatoren sein. Ein Rückblick auf die Bilanz der letzten europäischen Legislaturperiode zeigt klar, dass sich Europa in den vergangenen 5 Jahren in die falsche Richtung bewegt hat.

Heterogenität als Schlüssel zur Resilienz

Ein vielfältiges Ökosystem ist Grundpfeiler für ein widerstandsfähiges Finanzsystem. Die Diversität von Technologien, Geschäftsmodellen und Denkweisen trägt dazu bei, Risiken zu verteilen und unvorhergesehene Herausforderungen besser bewältigen zu helfen. Indem wir Heterogenität fördern, schaffen wir eine natürliche Barriere gegen Störungen und erhöhen die Fähigkeit, uns an Veränderungen anzupassen. Gerade Österreich hat den Vorteil, eines heterogenen und damit auf vielen Erfolgspfeilern stehenden Finanzmarkts. Dies gilt es anzuerkennen und zu schützen.



Der Weg nach vorne

Was bedeutet all dies für die Zukunft? Zunächst müssen wir wohl erkennen, dass Finanzresilienz eine gemeinsame Verantwortung ist. Staatliche, zivilgesellschaftliche und private Akteure müssen zusammenarbeiten, um Lösungen zu entwickeln, die den Anforderungen unserer Zeit gerecht werden. Politische Entscheidungsträger müssen mutig genug sein, die Illusion der Kontrolle zu durchbrechen und die Realität der Risiken anzuerkennen. Dies kann aber nicht allein Aufgabe der Politik sein, sondern alle Menschen sind in die Verantwortung zu nehmen. Zugleich müssen sie aber auch den Weg für Innovation und Flexibilität ebnen.

Die Veröffentlichung des Whitepapers von Mastercard Österreich ist auch in diesem Kontext ein wesentlicher Schritt in diese Richtung. Durch die Zusammenarbeit von Experten aus Wirtschaft, Wissenschaft und Politik können wir Strategien entwickeln, die die Finanzresilienz stärken. Das Ziel ist klar: Ein Finanzsystem, das stabil ist, sich den Turbulenzen unseres Multikrisenumfeldes entgegenstellt und flexibel genug ist, um neue Chancen zu nutzen. Indem wir die Herausforderungen als Möglichkeiten betrachten, ebnen wir gemeinsam den Weg für stabile Lösungen und eine widerstandsfähige, resiliente Zukunft.

Mag. Dr. Valeska Grond-Szucsich LL.M.
Leitung Bereich Verbraucherangelegenheiten und Datenschutz, Verband österreichischer Banken & Bankiers

Regulatorik und ihre Auswirkungen auf die Finanzresilienz am Beispiel der Europäischen Datenstrategie

Finanzresilienz – Was ist das?

Spricht man von „Finanzresilienz" geht es um die Fähigkeit einer Volkswirtschaft, der wirtschaftlichen, politischen, technologischen und gesellschaftlichen Entwicklung erfolgreich zu begegnen. Eine resiliente Volkswirtschaft ist auf Krisen vorbereitet, ohne sich dabei selbst durch die Angst vor einer Krise zu lähmen. Vielmehr kann sie auf die durch Veränderungen im Umfeld (die nicht steuerbar sind) verursachten Herausforderungen erfolgreich reagieren und den sich ändernden Rahmenbedingungen gerecht werden.

Wie trägt der Gesetzgeber zur Finanzresilienz bei?

Einen wichtigen Beitrag zur Resilienz von Volkswirtschaften leistet der Gesetzgeber. Regulatorik hat eine Steuerungsfunktion, die sich sofort im Alltag unmittelbar in der tatsächlichen Ausgestaltung von Lebensbereichen zeigt. Eine resiliente Volkswirtschaft bietet ein stabiles Finanz- und Wirtschaftssystem, das offen gegenüber Neuerungen (wie z. B. der Öffnung des Wirtschaftstandortes für erneuerbare Energie und Innovationen) und der Schaffung einer sicheren Lebens- und Entwicklungsumgebung für die Bevölkerung ist. Der einzelne Mensch entscheidet durch sein tägliches Verhalten darüber, wie erfolgreich die regulatorischen „Resilienzmaßnahmen" tatsächlich sind.

Daten, Digitalisierung und Künstliche Intelligenz

Digitalisierung und der Umgang mit Künstlicher Intelligenz gehören aktuell zu den ganz großen Themen der Finanzbranche. Die Corona-Krise hat den Trend zur Digitalisierung deutlich verstärkt und das Konsumentenverhalten hat sich grundlegend verändert. Die Digitalisierung der Finanzbranche hat weit früher begonnen, was nicht nur auf wirtschaftliche Überlegungen (Automatisierung von Prozessen, höhere Geschwindigkeit der Dienstleistung, verbesserte Betrugsbekämpfung, etc.), sondern auch auf regulatorische Vorgaben zurückzuführen ist. Hier sei als Beispiel angeführt, dass der Europäische Gesetzgeber in der ersten Zahlungsdiensterichtlinie („RL 2007/64/EG", „PSD 1") festgelegt hat, wie lange eine Überweisung längstens dauern darf. Um diese Erledigungsfrist zu schaffen, haben Zahlungsdienstleister den Prozess zur Erledigung von Zahlungsaufträgen gänzlich automatisiert und digitalisiert. Dieses Beispiel steht stellvertretend für viele Bereiche, in denen der Regulator die Digitalisierung rasch vorangetrieben hat.

In unserer (zunehmend) digitalisierten Welt werden Daten und ihre Verarbeitung, Analyse und Verwendung immer wichtiger. Der Titel eines Economist-Artikels vom 6. Mai 2017 lautet „The world's most valuable resource is no longer oil, but data" [2] – diese Headline fasst den gesamten Artikel, in dem es um die gestiegene und weiterhin wachsende wirtschaftliche Macht von Daten geht, zusammen. Heute findet man immer wieder Anlehnungen an diesen Artikel, z.B. in dem Daten als das Öl des 21. Jahrhunderts [3] bezeichnet werden. Die Ressource Öl wird jedoch bei einmaliger Nutzung verbraucht, Daten nicht.

Die Rolle der Big Techs

Big Techs wie Apple, Amazon, Google, Microsoft und Meta, schaffen Fakten, die oftmals lediglich zu einer Reaktion der Politik und der anderen Wirtschaftsteilnehmer führen. Nicht alle Projekte der Big Techs führen direkt zum Erfolg – man denke z. B. an die LIBRA von Facebook – doch der Einfluss der Big Techs sowie ihrer Ideen und Projekte ist unumstritten.

Diese Unternehmen haben Trends wie jene zu Big Data und zur Künstlichen Intelligenz früh aufgegriffen und nicht darauf gewartet, was der Regulator erlaubt. Die Regulatoren, zeitlich hinter diesen technischen und wirtschaftlichen Entwicklungen, können teilweise lediglich auf die geschaffene neue Situation reagieren und eine Regulierung im Nachhinein auf den Weg bringen.

Datennutzung und Wirtschaftlicher Erfolg

Der überlegte Umgang mit Daten bringt Unternehmen deutliche Wettbewerbsvorteile. Die alte Weisheit „Wissen ist Macht" gilt gerade auch im Umgang mit Daten: Je mehr Daten ein Unternehmen sinnvoll verarbeitet, speichert und analysiert, desto besser kann es einerseits auf aktuelle Entwicklungen reagieren und andererseits mögliche künftige Entwicklungen vorausberechnen.

Heute (mit den bereits bestehenden Möglichkeiten der Künstlichen Intelligenz und dem Potenzial der Verwendung bestehender Daten im Hinblick auf Data Science, Machine Learning und mehr) werden Daten immer mehr zu einer wertvollen Ressource. Durch die Möglichkeiten der Datennutzung tun sich immer neue Anwendungsfälle für den gewinnbringenden Einsatz von Daten auf. Die erfolgreiche Verwendung von Daten ist branchenübergreifend und zeigt sich von der Medizin über die öffentliche Verwaltung bis zu ihrem Einsatz in der Produktenwicklung. Sollte die Wichtigkeit der Ressource „Daten" übersehen werden, wird dies vermutlich zu einem Misserfolg führen.

Wie kann der Regulator im Hinblick auf diese Entwicklung zur Resilienz beitragen?

Die EU-Kommission sieht die wirtschaftliche Bedeutung von Daten in einer zunehmend digitalisierten Welt und hatte sich daher zum Ziel gesetzt, den Umgang mit Daten gesetzlich zu regeln. Um dieses Ziel zu erreichen, wurde die „Europäische Datenstrategie" entwickelt und umgesetzt. Daten bezeichnet die EU-Kommission als „eine wesentliche Ressource für Wirtschaftswachstum,

Wettbewerbsfähigkeit, Innovation, die Schaffung von Arbeitsplätzen und den gesellschaftlichen Fortschritt im Allgemeinen".[4]

Die europäische Datenstrategie dient dazu, „einen Binnenmarkt für Daten zu schaffen, der die globale Wettbewerbsfähigkeit und Datensouveränität Europas sichert. Die Führungsrolle der EU in der globalen Datenwirtschaft soll weiter gestärkt werden."[5]

Der Regulator unterstützt hiermit die Resilienz der europäischen Volkswirtschaften, in welchen immer mehr Datennutzung erfolgt und die sich im globalen Wettbewerb befinden.

Datenschutz is key – Kluge Datennutzung ebenfalls

Die EU-Kommission bekennt sich dazu, „den Menschen bei der Entwicklung von Technologien an die erste Stelle zu setzen und die europäischen Werte und Rechte in der digitalen Welt zu verteidigen und zu fördern".[6]

Die DSGVO dient dem Schutz personenbezogener Daten. Neben die DSGVO treten der Data Act[7] und der Data Governance Act („DGA")[8].

Die Vorgaben des Data Act sollen es möglich machen, das Potenzial der ständig wachsenden Menge an Industriedaten zu nutzen. Der Data Governance Act (DGA) regelt die Wiederverwendung von öffentlichen oder geschützten Daten in verschiedenen Sektoren sowie deren Überwachung.

Der europäische Regulator beabsichtigt, mit dem Data Act und dem DGA das Vertrauen in die gemeinsame Nutzung und Wiederverwendung von Daten zu stärken[9]. Die Hintergrundidee ist, das Vertrauen der Marktteilnehmer dahingehend zu stärken, dass die Verfügbarkeit von Daten auf dem Markt erhöht wird, wodurch wiederum auch die Möglichkeit zur Datennutzung steigt. Unternehmen und Einzelpersonen, die die Daten erzeugen, behalten bei diesem Prozess die Kontrolle. Dieses gesetzliche Konzept soll eine verbesserte und vermehrte Datennutzung bei gleichzeitigem Vertrauen der Marktteilnehmer in den legal funktionierenden Markt ermöglichen.

DSGVO, Data Act und DGA in a nutshell

Die DSGVO schützt personenbezogene Daten. Sie erlaubt die Verarbeitung personenbezogener Daten grundsätzlich nur unter Voraussetzung der Einhaltung bestimmter Grundsätze.

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Die DSGVO normiert weiters die Grundsätze der Zweckbindung, der Datenminimierung, der Richtigkeit der Datenverarbeitung, der Speicherbegrenzung sowie der Integrität und Vertraulichkeit. Der jeweilige Verantwortliche muss die Einhaltung dieser Grundsätze nachweisen können, ihn trifft somit eine Rechenschaftspflicht.

Personenbezogene Daten dürfen nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit ebendieser bietet. Geeignete technische und

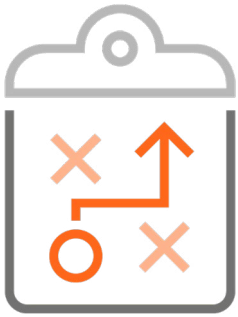
organisatorische Maßnahmen sollen sicherstellen, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

Dazu sollen Data Act und DGA einen rechtlichen Rahmen für die faire und wirtschaftlich sinnvolle Verwendung von Daten bieten und dadurch einen Beitrag zur Stärkung der Wirtschaft und der Resilienz der europäischen Volkswirtschaften leisten.

Der branchenübergreifend geltende Data Act regelt den Austausch und die gemeinsame Nutzung von nicht personenbezogenen Daten. Das betrifft z.B. die Verwendung vernetzter Produkte oder damit verbundener Dienste im Internet der Dinge. Das Recht auf Datenübertragbarkeit wird geregelt und das Kopieren oder Übertragen von Daten aus verschiedenen Diensten wird erleichtert. Mehr Datennutzung soll zu mehr Wertschöpfung führen - insbesondere auch vor dem Hintergrund der Nutzung von KI.

Geregelt werden im Data Act die Datenweitergabe von Unternehmen an Verbraucher (B2C) und zwischen Unternehmen (B2B) sowie der Pflichten der Dateninhaber zur Datenbereitstellung. Weiters wird geregelt, welche Vertragsklauseln nicht für den Datenzugang und die Datennutzung zwischen Unternehmen (B2B) vereinbart werden dürfen. Zudem gibt es Vorschriften über die Bereitstellung von Daten für öffentliche Stellen wegen außergewöhnlicher Notwendigkeit (B2G) und Vorgaben zu vertraglichen Regelungen und der technischen Umsetzung beim Wechsel zwischen Datenverarbeitungsdiensten („Cloud Switching").

Der Data Governance Act ist ein sektorübergreifendes Instrument und reguliert die Wiederverwendung von öffentlichen, geschützten Daten, indem der Datenaustausch durch die Regulierung neuartiger Datenintermediäre erleichtert und der Austausch von Daten zu altruistischen Zwecken gefördert wird. In seinen Geltungsbereich fallen sowohl personenbezogene als auch nicht personenbezogene Daten. Für alle personenbezogenen Daten gilt zudem die Datenschutz-Grundverordnung (DSGVO).



Fazit

Es bleibt abzuwarten, wie erfolgreich die Europäische Datenstrategie in der Praxis sein wird, insbesondere im Hinblick auf die mit ihr verbundene Bürokratie und die tatsächliche Förderung des Wirtschaftsstandortes Europa. Anzuerkennen ist jedoch jedenfalls die Idee der Förderung des Wirtschaftswachstums, der Innovation und der Wettbewerbsfähigkeit unter Priorisierung des Menschen und der Aufrechterhaltung von ausdrücklich als europäisch bezeichneten Werten und Rechten in der digitalen Welt. Der europäische Gesetzgeber hat hier eine Chance gesehen, die (Finanz-) Resilienz der europäischen Volkswirtschaften zu stärken. Gerade im Bereich der Datenverarbeitung und -analyse ist die technische Entwicklung rasant. Um die Resilienz weiterhin zu stärken ist es notwendig, die technische Entwicklung im Kontext mit der Verwendung von Daten genau zu beobachten und - wenn nötig - auch den rechtlichen Rahmen weiterzuentwickeln. Denn auch veraltete Regelungen können die Resilienz schwächen. Zentral ist es, die Krisentragfähigkeit zu stärken und für die Zeit nach der Krise bestmögliche Wachstumsbedingungen zu schaffen.

4. Payments & Cybersecurity

Maja Hoffmann
ehemals Head of Anti-Fraud Management, Unicredit

Resilienz und Betrugsabwehr im digitalen Zeitalter

Die Gewährleistung und Sicherstellung von Resilienz im Finanzsystem ist heute von entscheidender Bedeutung, insbesondere im Hinblick auf Sicherheits- und Betrugsthemen. In einer Welt, die zunehmend von technologischen Fortschritten und geopolitischen Spannungen geprägt ist, müssen Regulatorik, Wirtschaft und Gesellschaft gemeinsam darauf hinarbeiten, eine robuste Finanzinfrastruktur zu schaffen. Der Zahlungsverkehr und der Schutz der Identität als neue Währung stehen hierbei besonders im Fokus.

Jeder Dienstleister, jedes Produkt, jede Identität und jedes gesellschaftliche Ereignis kann in der heutigen Zeit für kriminelle und destabilisierende Zwecke verwendet werden. Akteure verschiedener Industrien, Dienstleister und Behörden werden seitens krimineller Elemente gegeneinander ausgespielt. Legitime Angebote (wie z.B. das Schalten von Werbung auf öffentlichen digitalen Plattformen) werden mit großer Leichtigkeit für gefälschte Inhalte herangezogen. Markenmissbrauch, Amtsanmaßung und Identitätsdiebstahl sind verbreiteter denn je.

Herausforderungen und Chancen im technologischen Fortschritt

In unserer schnelllebigen Zeit bringt der technologische Fortschritt sowohl Chancen als auch Herausforderungen für Zahlungsdienstleister mit sich. Die Integration neuer Technologien kann die Effizienz und Sicherheit des Zahlungsverkehrs erheblich verbessern. Allerdings gehen diese Technologien auch mit neuen Risiken einher, die es zu bewältigen gilt.

Ein Beispiel dafür ist die Künstliche Intelligenz. Während KI-Systeme dazu verwendet werden können, Betrugsmuster zu erkennen und Angriffe abzuwehren, werden sie ebenso von Kriminellen genutzt. Der Leitsatz „Ich glaube nur das, was ich sehe" ist in einer Welt, in der Bild- und Tonmaterial innerhalb kürzester Zeit künstlich generiert werden können, obsolet geworden. Jedes Gesicht und jede Stimme können simuliert und dazu verwendet werden, Menschen zu beeinflussen und Chaos zu stiften.

Dadurch soll aber kein negatives Bild von neuen Technologien entstehen. Schließlich kann jedes Werkzeug mit konstruktiver oder destruktiver Absicht verwendet werden. Schnelligkeit, Benutzerfreundlichkeit und Sicherheit sind Kernthemen, die durch die Hilfe neuer Technologien unterstützt werden können. Zahlreiche innovative Lösungen ermöglichen die Verbesserung vieler Dienstleistungen.

Die Integration neuer Technologien erfordert jedoch eine kontinuierliche Anpassung der regulatorischen Rahmenbedingungen. Regierungen und Aufsichtsbehörden stehen vor der Aufgabe, ein Gleichgewicht zwischen Innovation und Sicherheit zu finden. Dies beinhaltet auch die Schaffung von Standards für neue Technologien und Dienstleister.

Die Bedrohung durch Cyberkriminalität und die Notwendigkeit der Zusammenarbeit

Kriminelle Organisationen nutzen jede verfügbare Infrastruktur, um sich zu bereichern oder Chaos zu stiften. In einer digital vernetzten Welt müssen alle Akteure Verantwortung übernehmen und eng zusammenarbeiten, um diesen Bedrohungen entgegenzuwirken. Angriffe auf Privatpersonen, Krankenhäuser und andere Institutionen nehmen in ihrer Aggressivität und Raffinesse zu. Die kriminelle Landschaft ist hochorganisiert und hat oft ähnliche Strukturen wie legale Unternehmen, hält sich jedoch weder an Grenzen noch Gesetze und verfügt darüber hinaus oft über unlimitierte Ressourcen.

Sicherheit ist nicht länger nur ein Expertenthema. Die Zusammenführung der Cyberkriminalität und technischen Mitteln mit klassischen Betrugsmustern führt zu einer erhöhten Notwendigkeit an Basiskompetenz jedes Einzelnen. So wie Kernelemente im Alltag, z.B. „Gehe nicht bei Rot über die Straße" oder „Nimm keine Süßigkeiten von Fremden an", werden Regeln für den Umgang mit dem Internet bereits in der Grundschule angesprochen. Auch Eltern stehen im Bestreben, für die Sicherheit ihrer Kinder zu sorgen, vor bisher nie dagewesenen Herausforderungen.

Fazit

Um kriminellen Machenschaften den Riegel vorzuschieben, ist eine Gesamtverantwortung und ein gemeinsames, konsolidiertes und gesetzlich klar definiertes Rahmenwerk notwendig, das auf einem klaren Verständnis der Problematik basiert. Undeutlichkeiten und regional diversifizierte Auslegungen von Datenschutzregeln stellen eine signifikante Barriere zur inter- und intra-Sektor-Kollaboration dar.

Durch die enge Zusammenarbeit aller Akteure, die kontinuierliche Anpassung an technologische Entwicklungen und die Schaffung eines stabilen regulatorischen Rahmens kann die Resilienz gestärkt und die Sicherheit von Staat, Wirtschaft und Gesellschaft gewährleistet werden. Eine unmissverständlich bewilligte Infrastruktur zur Kollaboration ist unerlässlich, um die stetig wachsenden Bedrohungen durch Cyberkriminalität effektiv zu bekämpfen.

Zu Strafbarkeitsrisiken des Opfers von Ransomware-Erpressungen bei Zahlung eines Erpressungsbetrags und wie man diesen vorbeugt

Mag. Dr. Norbert Wess
LL. M., MBL, Rechtsanwalt und Partner bei wkk law Rechtsanwälte in Wien und Wirtschaftsstrafrechtsexperte

Mag. Markus Machan
Rechtsanwalt bei wkk law Rechtsanwälte in Wien spezialisiert auf Finanzstrafrecht, Verwaltungsstrafrecht, Wirtschaftsstrafrecht und Unternehmensrecht

Allgemeines

Im letzten Jahr sind in Österreich wiederholt Fälle von Ransomware-Erpressungen bekannt geworden. Dabei infizieren die Täter die Computersysteme der betroffenen Unternehmen zunächst mit einem Trojaner, welcher die Daten der Opfer verschlüsselt, und fordern diese im Anschluss auf, für die Entsperrung der Daten einen – zumeist nicht unbeträchtlichen – Geldbetrag zu zahlen.

Diese Täter von Ransomware-Erpressungen haben in den allermeisten Fällen eine Datenbeschädigung nach § 126a StGB zu verantworten. Danach macht sich strafbar, wer einen anderen dadurch schädigt, dass er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt. In Betracht kommt darüber hinaus eine Strafbarkeit wegen Störung der Funktionsfähigkeit eines Computersystems gemäß § 126b StGB und Missbrauch von Computerprogrammen oder Zugangsdaten gemäß § 126c StGB. Ob die Forderung des Lösegeldes eine Erpressung nach § 144 StGB oder eine Nötigung gemäß § 105 StGB konstituiert, hängt nach der hL einerseits vom Verhältnis zwischen der Höhe des geforderten Lösegeldes und dem tatsächlichen Wert der Daten und andererseits vom Vorliegen des Schädigungsvorsatzes ab. Der OGH würde die Verwirklichung des Tatbestandes der Erpressung nach § 144 StGB hingegen jedenfalls bejahen. Schließen sich mehrere Täter zur Begehung des Ransomware-Angriffes bzw der nachfolgenden Erpressung zusammen, kommt immer auch eine Strafbarkeit nach dem Organisationsdelikt der kriminellen Vereinigung gemäß § 278 StGB in Betracht.

Strafbarkeit des Opfers bei Zahlung des Erpressungsbetrags bzw. bei Beteiligung daran?

Die Erfahrung und Statistiken zeigen, dass betroffene Unternehmen trotz entsprechender Warnungen seitens der Behörden dazu neigen, den Forderungen der Erpresser nachzukommen und das Lösegeld für die Entsperrung der Daten zahlen. Diese Zahlungen bergen aber auch ein Strafbarkeitsrisiko für die Opfer selbst, wobei wie folgt zu unterscheiden ist:

Handelt es sich bei dem Täter des Ransomware-Angriffs um einen Einzeltäter, besteht für das Opfer bei Zahlung des Erpressungsbetrages kein Strafbarkeitsrisiko.

Handelt es sich jedoch um mehrere Täter und agieren diese im Rahmen einer kriminellen Vereinigung iSd § 278 StGB, kann sich – bei Vorliegen eines entsprechenden Vorsatzes – grundsätzlich auch das Opfer durch die Zahlung des geforderten Geldbetrages nach dieser Bestimmung strafbar machen, weil es die kriminelle Vereinigung durch das Zurverfügungstellen von Vermögenswerten oder auf andere Weise fördert.

Eine kriminelle Vereinigung ist nach § 278 Abs 2 StGB *„ein auf längere Zeit angelegter Zusammenschluss von mehr als zwei Personen, der darauf ausgerichtet ist, dass von einem oder mehreren Mitgliedern der Vereinigung ein oder mehrere Verbrechen, andere erhebliche Gewalttaten gegen Leib und Leben, nicht nur geringfügige Sachbeschädigungen, Diebstähle oder Betrügereien, Vergehen nach den §§ 177b, 233 bis 239, 241a bis 241c, 241e, 241f, 283, 304 oder 307, in § 278d Abs 1 genannte andere Vergehen oder Vergehen nach den §§ 114 Abs 1 oder 116 des Fremdenpolizeigesetzes ausgeführt werden."* Damit eine kriminelle Vereinigung iSd § 278 StGB vorliegt, bedarf es daher mindestens drei Täter, die mit einer kriminellen Zielsetzung längere Zeit hindurch zusammenwirken.

Gemäß § 278 Abs 3 StGB beteiligt sich derjenige an einer kriminellen Vereinigung *„wer [...] sich an ihren Aktivitäten durch die Bereitstellung von Informationen oder Vermögenswerten oder auf andere Weise in dem Wissen beteiligt, dass er dadurch die Vereinigung oder deren strafbare Handlungen fördert."*

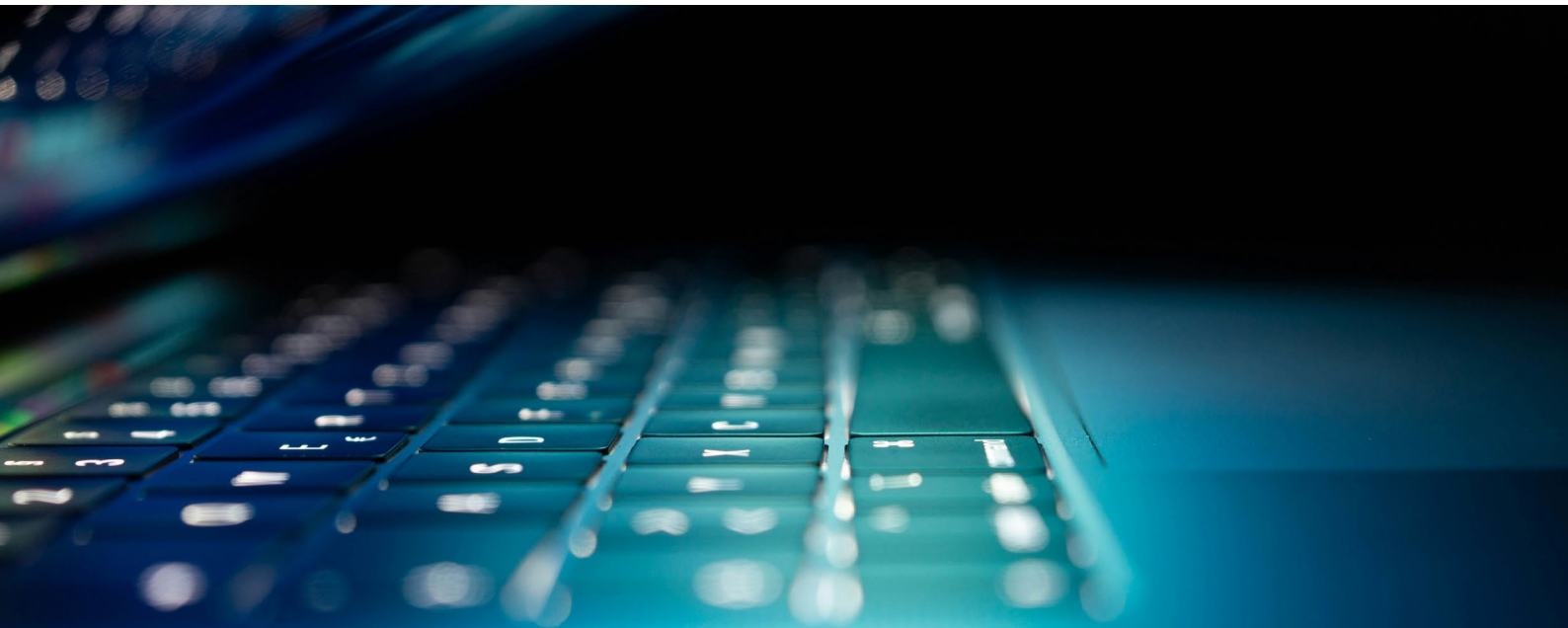
Angesichts des Wortlauts der Legaldefinition in Abs 3 leg cit beteiligt sich daher bereits jeder, der eine Beteiligungshandlung iSd Abs 3 leg cit mit dem dort geforderten Vorsatz setzt, als Mitglied an einer kriminellen Vereinigung. Auf eine eigenständige objektiv und von etwaigen Beteiligungshandlungen losgelöste Mitgliedschaft in einer kriminellen Vereinigung kommt es nicht an. Dies führt zu dem Ergebnis, dass sich sogar das Erpressungsopfer wegen Beteiligung an einer kriminellen Vereinigung als Mitglied nach § 278 Abs 1 zweiter Fall StGB strafbar machen kann.[10] In der Rsp zeigt sich dies insoweit, dass diese einerseits auf eine separate Prüfung der Mitgliedschaft verzichtet[11] und andererseits der OGH in einem *obiter dictum* ausdrücklich ausgesprochen hat, dass bereits jede wissentliche Förderung einer kriminellen Vereinigung die Mitgliedschaft iSd § 278 Abs 3 StGB begründet.[12] In der Literatur wird hingegen auch eine einschränkende Auslegung des § 278 StGB vertreten.[13]

Für das Erpressungsopfer, welches die finanziellen Mittel für die Lösegeldzahlung bereitstellt, ist in einem solchen Fall grundsätzlich die Handlungskategorie des Abs 3 zweiter Fall leg cit einschlägig („Bereitstellung von Vermögenswerten"). Vermögenswerte iSd Abs 3 leg cit sind jegliche Art von Vermögensgegenständen ungeachtet ihrer Art des Erwerbs.[14] In Betracht kommen in erster Linie Geldzuwendungen, aber auch Zuwendungen in Form von Kryptowährung oder andere Gegenstände. Eine Erheblichkeitsschwelle sieht Abs 3 zweiter Fall nicht vor.[15] Eine Bestimmungs- oder Beitragstäterschaft zur Beteiligung als Mitglied durch Bereitstellung von Vermögenswerten stellt im Hinblick auf die ihrerseits damit verbundene organisations- oder deliktsbezogene Förderung eine Beteiligung auf andere Weise iSd Abs 1 zweiter Fall iVm Abs 3 dritter Fall dar.[16]

Zur gebotenen Reduzierung des Strafbarkeitsrisikos für das Opfer

Das obengenannte Strafbarkeitsrisiko wird aber durch folgende Umstände reduziert:

§ 278 Abs 1 StGB ist ein Vorsatzdelikt. Bei der Begehungsform *„sich an einer kriminellen Vereinigung als Mitglied beteiligen"* (Abs 1 zweiter Fall leg cit) muss sich der Eventualvorsatz des Täters – hier: des Erpressungsopfers – auf die Existenz einer kriminellen Vereinigung und deren kriminelle Ausrichtung erstrecken. Die Handlungsalternativen der Beteiligung an einer kriminellen Vereinigung durch die Bereitstellung von Informationen oder Vermögenswerten oder auf andere Weise (Abs 1 zweiter Fall iVm Abs 3 zweiter und dritter Fall leg cit) erfordern in subjektiver Hinsicht zudem sogar Wissentlichkeit hinsichtlich der organisationsbezogenen oder deliktsbezogenen Förderung. Erst diese gesteigerte Vorsatzform konstituiert das Unrecht. Der Täter muss es also im Zeitpunkt der Vornahme einer dieser Beteiligungshandlungen für gewiss halten, dass er dadurch die kriminelle Vereinigung als solche und/oder strafbare Handlungen fördert.[17]



Liegen dem Erpressungsopfer zum Zeitpunkt der Zahlung des Erpressungsbetrages keine Hinweise vor, dass die Ransomware-Erpressung nicht in der Verantwortung einer kriminellen Vereinigung iSd § 278 StGB erfolgt, wird es in aller Regel an einem – strafbarkeitsbegründenden – Eventualvorsatz mangeln. Darüber hinaus wird es in einem solchen Fall naturgemäß auch an dem erweiterten Vorsatz mangeln, dass durch die Zahlung des Erpressungsbetrages eine kriminelle Vereinigung oder deren strafbare Handlung gefördert wird.

Vor diesem Hintergrund kommt einer entsprechend ausführlichen und detaillierten Dokumentation des Informationsstandes des Opfers im Zusammenhang mit der Vorbereitung und Durchführung der Zahlung – auf welchem Wege auch immer – für den Fall einer *ex post*-Betrachtung des Sachverhaltes eine ganz wesentliche Bedeutung zu. Gerade die subjektive Tatseite kann zumeist bloß aus objektiven Beweisen abgeleitet werden, weshalb diesen in einem allfälligen späteren Strafverfahren besonderes Augenmerk geschenkt wird.

Muss das Opfer – allenfalls aufgrund der Kommunikation mit den Tätern, allgemein zugänglicher Informationen über weit verbreitete Angriffe oder konkreter Nachforschungen im Zusammenhang mit dem Angriff – jedoch davon ausgehen, dass hinter dem Angriff eine kriminelle Vereinigung steckt, wird bei Zahlung des Erpressungsbetrages in aller Regel der objektive wie subjektive Tatbestand erfüllt sein. Allerdings bedeutet dies nicht zwangsläufig auch eine Strafbarkeit nach § 278 StGB. Es ist nämlich in derartigen Konstellationen stets zu prüfen, ob ein entschuldigender Notstand vorliegt, der einer Strafbarkeit entgegensteht.[18] Ob ein solcher vorliegt, ist aber jeweils im Einzelfall festzustellen.

Der entschuldigende Notstand setzt einen unmittelbar drohenden, bedeutenden Nachteil für ein Individualrechtsgut voraus. Dies ist im Falle eines Ransomware-Angriffs mit anschließender Erpressung zu bejahen. Der Handelnde ist dann gemäß § 10 StGB entschuldigt, wenn der Schaden aus der Tat (Förderung der kriminellen Vereinigung als solche und/oder deren strafbare Handlungen) nicht unverhältnismäßig schwerer als der abzuwendende Nachteil wiegt und von einem maßgerechten, mit den rechtlich geschützten Werten verbundenen Menschen kein anderes Verhalten zu erwarten wäre. Es ist daher zu prüfen, ob sich die Maßfigur in der konkreten Fallkonstellation für die Zahlung des Erpressungsbetrages (und gegen ein schonenderes Mittel, wie z. B. die Verwendung eines Backups) entschieden hätte. Dies könnte mitunter dann vorliegen, wenn die selbstständige Wiederherstellung mit enormem Zeitaufwand verbunden wäre, der Inhalt der verschlüsselten Daten jedoch sofort benötigt wird. Besteht wiederrum kein Backup, wird der Wert der betroffenen Daten sowie der für ihre Neuerstellung verursachte Aufwand in die Abwägung miteinzubeziehen sein. Stets ist dabei jedoch auch die Wahrscheinlichkeit der tatsächlichen Entsperrung der Daten zu berücksichtigen.[19] Wäre bereits bekannt, dass die Angreifer die Daten trotz Zahlung des Lösegeldes nicht wieder entschlüsseln, würde dies die Anwendbarkeit des § 10 StGB ausschließen.

Es ist daher ausdrücklich darauf hinzuweisen, dass einer ausführlichen Falldokumentation entscheidende Bedeutung zukommt, welche die oben angeführten, vom Erpressungsopfer zwingend anzustellenden Abwägungen und Überlegungen bei einer späteren ex-post Betrachtung durch Dritte (wie bspw. Strafverfolgungsbehörden) zugänglich und nachvollziehbar machen.

Eine Rechtfertigung kraft rechtfertigenden Notstandes kommt nicht in Betracht. Denn selbst wenn eine Notstandssituation zu bejahen ist und die Notstandshandlung das schonendste Mittel zur Rettung eines höherwertigen Rechtsgutes ist, kann sich das Erpressungsopfer nicht erfolgreich auf den rechtfertigenden Notstand stützen, wenn die Tat – bezogen auf die obersten Prinzipien und Wertbegriffe der Rechtsordnung – nicht als angemessen beurteilt werden kann.[20] Nach der herrschenden Meinung in der Literatur wird dieses Angemessenheitskorrektiv in solchen Konstellationen verletzt, in denen jemand eine Straftat gezwungener Maßen begeht, um einen sonst von dritter Seite drohenden Nachteil abzuwenden. Dies wird zum einen damit begründet, dass die Beeinträchtigung des fremden Rechtsguts nicht zur unmittelbaren Bewahrung der eigenen Interessen führt, sondern bloß die Voraussetzungen dafür schafft, dass der Angreifer die Bedrohung der eigenen Rechtsgüter aufgibt.[21] Andererseits wäre es nach diesen Literaturmeinungen aus sozialethischen Gesichtspunkten inakzeptabel, in den Fällen des Nötigungsnotstands ein Vorgehen des Genötigten aufgrund der Anwendbarkeit des rechtfertigenden Notstands als rechtmäßig anzusehen, zumal sich unbeteiligte Dritte, in deren Rechtsgüter durch den Genötigten eingegriffen wird, zum Schutz ihrer Rechte mangels Rechtswidrigkeit des Angriffs nicht auf das Notwehrrecht berufen könnten.[22]

(Technische) Unterstützung der Opfer von Ransomware-Erpressungen

Opfer von Ransomware-Angriffen benötigen oft rasche und spezialisierte technische Unterstützung, um den Vorfall zu bewältigen und die Auswirkungen zu minimieren. Diese Unterstützung umfasst verschiedene Maßnahmen, die sowohl präventive als auch reaktive Schritte beinhalten können, um den Schaden für das betroffene Unternehmen zu begrenzen.

Zu den häufigsten Maßnahmen gehören die Verhandlung mit den Erpressern, um Zeit für die Wiederherstellung der Systeme zu gewinnen oder das geforderte Lösegeld zu reduzieren. Dabei werden spezialisierte Verhandlungstechniken eingesetzt, die darauf abzielen, den Forderungsbetrag so weit wie möglich zu senken oder alternative Lösungen zu finden.

Ein weiterer wichtiger Aspekt ist die Durchführung einer rechtlich abgesicherten Lösegeldzahlung. Hierbei müssen strikte Prüfungen in Bezug auf Geldwäschegesetze und Sanktionen eingehalten werden, um sicherzustellen, dass weder das Unternehmen noch seine Entscheidungsträger durch die Zahlung selbst strafrechtliche Risiken eingehen.

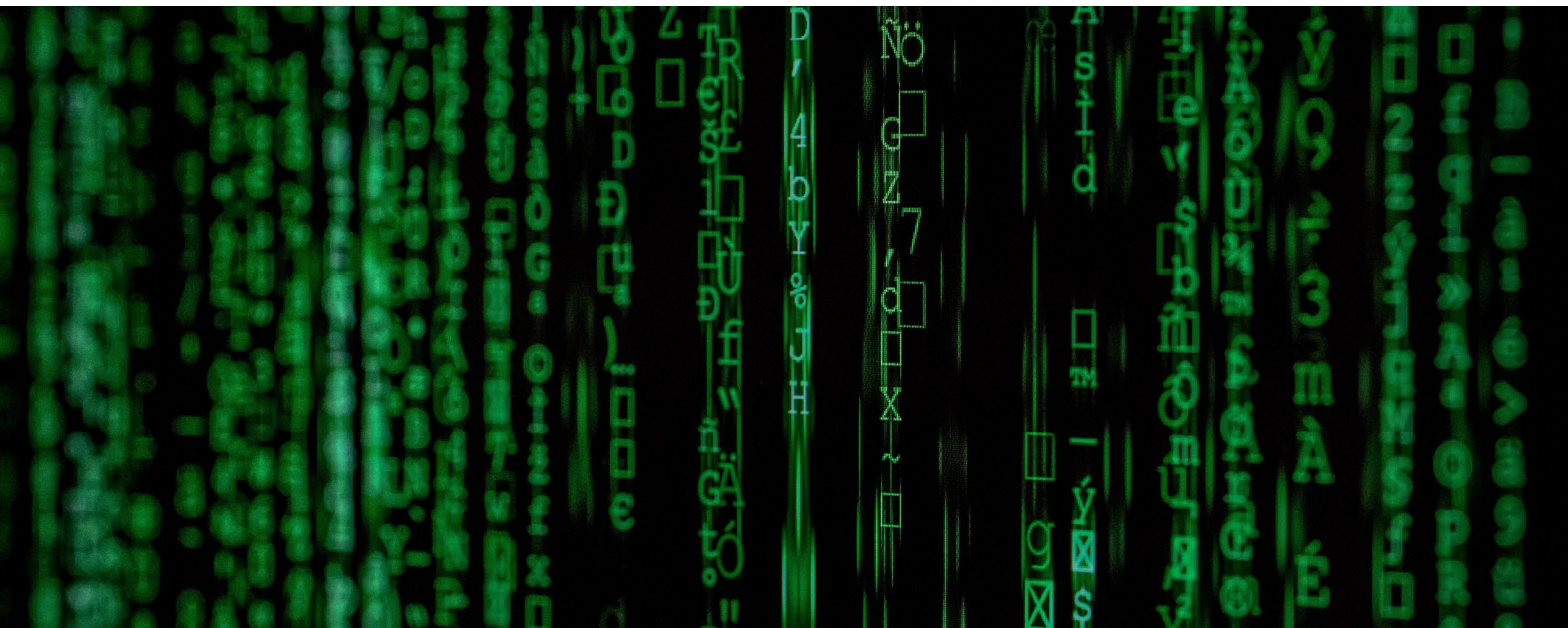
Die schnelle Bereitstellung von Kryptowährungen, die bei Ransomware-Erpressungen häufig als Zahlungsmittel gefordert werden, stellt einen wesentlichen operativen Schritt dar, um die Erfüllung von Forderungen innerhalb der gesetzten Fristen zu ermöglichen.

Parallel dazu wird oftmals ein Monitoring des Datenabflusses implementiert, um festzustellen, ob sensible Daten bereits exfiltriert oder verkauft wurden. Diese Maßnahme dient nicht nur dem Schutz des Unternehmens, sondern auch der Erfüllung der Pflichten gegenüber Datenschutzbehörden.

Nach der Zahlung des Lösegelds können spezialisierte Verfahren zur Rückverfolgung der gezahlten Mittel zum Einsatz kommen. Diese Maßnahmen zielen darauf ab, die illegal erworbenen Gelder zu lokalisieren und rechtliche Schritte einzuleiten, um diese einzufrieren, bevor sie in andere Währungen umgewandelt oder verschleiert werden.

Zusammenfassung

Cyberkriminalität ist der am stärksten wachsende Bereich in der polizeilichen Anzeigenstatistik und stellt Unternehmen wie Privatpersonen vor enorme Herausforderungen. Dies gilt insbesondere für Ransomware-Erpressungen, bei denen den Opfern nicht nur ein erheblicher finanzieller Schaden, sondern in der Regel auch eine folgenreiche Zerstörung bzw. Einschränkung der IT-Systeme droht. Einer profunden rechtlichen und technischen Begleitung sowie der Unterstützung von Opfern derartiger Angriffe kommt daher besondere Bedeutung zu, um Schäden zu minimieren und allfälligen rechtlichen Risiken vorzubeugen.



QUELLENVERZEICHNIS

1. CybersecurityVentures; abgerufen am 09.11.2024
2. The world's most valuable resource is no longer oil, but data (economist.com), abgerufen am 09.08.2024.
3. Ein Beispiel für viele: "Daten – das Öl des 21. Jahrhunderts", Artikel der Tageszeitung „Die Presse" vom 21.6.2018, abgerufen am 09.08.2024.
4. Eine europäische Datenstrategie | Europas digitale Zukunft gestalten, abgerufen am 09.08.2024.
5. Eine europäische Datenstrategie | Europas digitale Zukunft gestalten, abgerufen am 09.08.2024.
6. Eine europäische Datenstrategie | Europas digitale Zukunft gestalten, abgerufen am 09.08.2024.
7. Die am 27. November 2023 verabschiedete „Verordnung (EU) 2023/2854 über Vorschriften für einen fairen Datenzugang und eine faire Datennutzung" (kurz: Data Act) tritt am 11. Januar 2024 in Kraft und wird ab dem 12. September 2025 EU-weit direkt anwendbares Recht.
8. Die „Verordnung (EU) 2022/868 über europäische Daten-Governance" (kurz: Data Governance Act, „DGA") trat am 23. Juni 2022 in Kraft und gilt nach Ablauf einer Nachfrist von 15 Monaten seit September 2023.
9. Eine europäische Datenstrategie | Europas digitale Zukunft gestalten, abgerufen am 09.08.2024.
10. Plöchl in WK-StGB2 § 278 Rz 38.
11. OGH 19.02.2009, 12 Os 152/08g.
12. OGH 17.12.2015, 12 Os 106/15b; ausführlich dazu Kahl/Stücklberger, Strafrechtliche Implikationen des „WannaCry"-Angriffes – aus Sicht von Tätern und Opfern, JSt 2018, 35.
13. Siehe im Detail Kahl/Stücklberger, JSt 2018, 35 f.
14. Plöchl in WK-StGB2 § 278 Rz 38
15. Plöchl in WK-StGB2 § 278 Rz 38.
16. Plöchl in WK-StGB2 § 278 Rz 39.
17. RIS-Justiz RS0124903; Plöchl in WK-StGB2 § 278 Rz 41.
18. Plöchl in WK-StGB2 § 278 Rz 38.
19. Kahl/Stücklberger, JSt 2018, 38.
20. Kahl/Stücklberger, JSt 2018, 37; Kienapfel, ÖJZ 1975, 429.
21. Kahl/Stücklberger, JSt 2018, 37; Lewisch in WK-StGB2 Nachbem zu § 3 Rz 101.
22. Kahl/Stücklberger, JSt 2018, 37 mit Verweis auf Kienapfel, ÖJZ 1975, 430, Lewisch in WK-StGB2 Nachbem zu § 3 Rz 101 und Steininger in SbgK Nachbem § 3 Rz 61.

IMPRESSUM

Herausgegeben von:

Mastercard Europe SA
Representative Office Austria

Wipplingerstrasse 30/DG
1010 Wien
Österreich
Vertretungsberechtigter: Michael Brönner

Mastercard Europe ist eine Tochtergesellschaft von Mastercard Incorporated, der Holding-Gesellschaft von Mastercard. Mastercard Incorporated ist eine private Aktiengesellschaft nach US-amerikanischem Recht und berichtet an die amerikanische Börsenaufsicht (SEC).
Mastercard Europe SA
Chaussée de Tervuren 198A
B-1410 Waterloo
Belgium
Vertretungsberechtigter: Mark Barnett
R.P.M (Registre des Personnes Morales) Nivelles, 0448.038.446
Mehrwertsteuer-Identifikationsnummer Mastercard Europe SA: TVA BE 0448.038.446.