ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

DIGITALE OPERATIONELLE RESILIENZ IM ZAHLUNGSVERKEHR

Alexander Natter, Anna Muri

Open Forum zum Thema Digitaler Euro und Zahlungsverkehr

26.06.2023

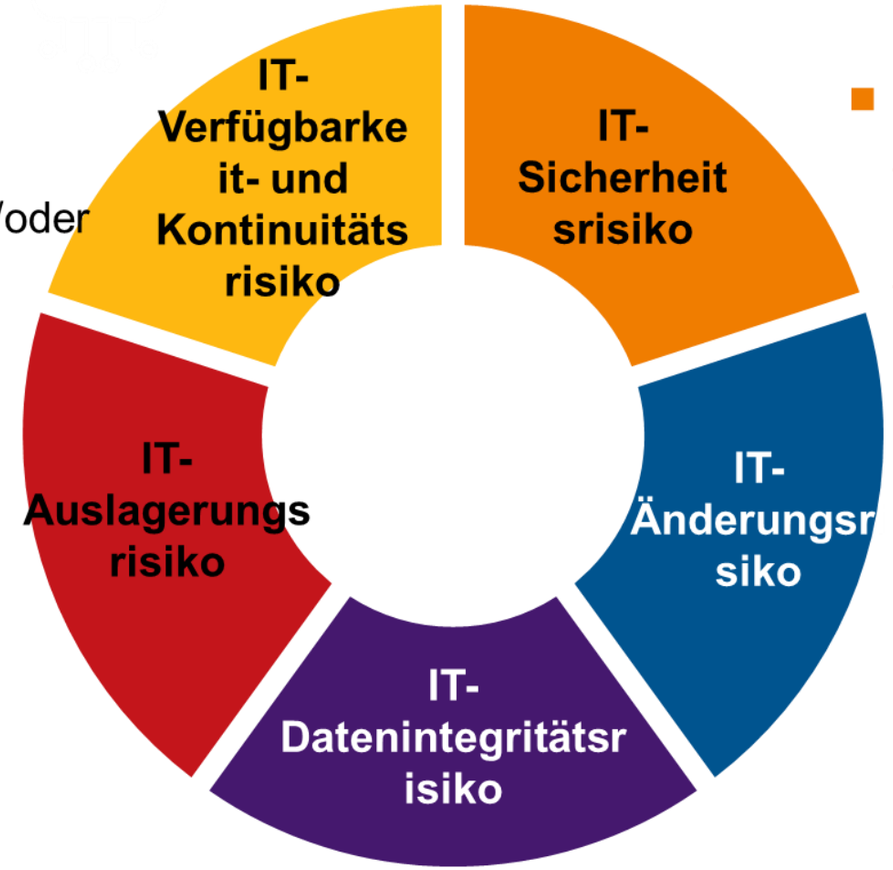
INHALTSVERZEICHNIS

- Was ist IT-Risiko und wie wird es beaufsichtigt?
- Warum ist die Begrenzung von IT-Risiken wichtig?
- Maßnahmen zur Begrenzung von IT- und operationellen Risiken im Zahlungsverkehr
- Die wichtigsten aufsichtlichen Regelungen

WAS IST IT-RISIKO UND WIE WIRD ES BEAUFSICHTIGT?

WAS IST IT-RISIKO?

- IT-Verfügbarkeits- und Kontinuitätsrisiko
  - Ausfall von Hardware und/oder Softwarekomponenten



- IT-Sicherheitsrisiko
  - Unbefugter Zugriff auf Systeme oder Daten
  - Cyberattacken

- IT-Auslagerungsrisiko
  - Unsicheres IT-Outsourcing

- IT-Änderungsrisiko
  - Keine (zeitgerechte) und kontrollierte Steuerung von IT-Systemänderungen möglich

- IT-Datenintegritätsrisiko
  - Unvollständige, ungenaue oder inkonsistente Daten

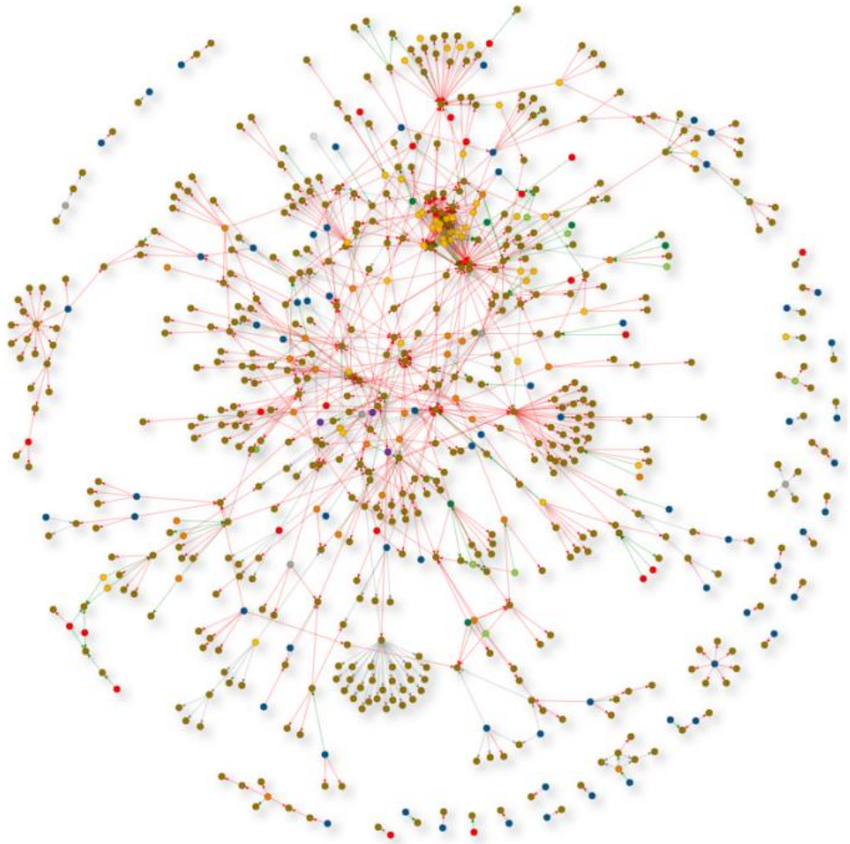
WIE WIRD IT-RISIKO BEAUFSICHTIGT?

AUF EINZELINSTITUTS-EBENE

- SREP: Supervisory Review and Evaluation Process
- IT-Vor-Ort-Prüfungen
- Managementgespräche/Einzelbankengespräche

AUF MAKRO-EBENE

- Cyber-Planspiel
- Digitalisierungsstudie
- Analyse Systembetreiber
- Benchmarking-Analysen



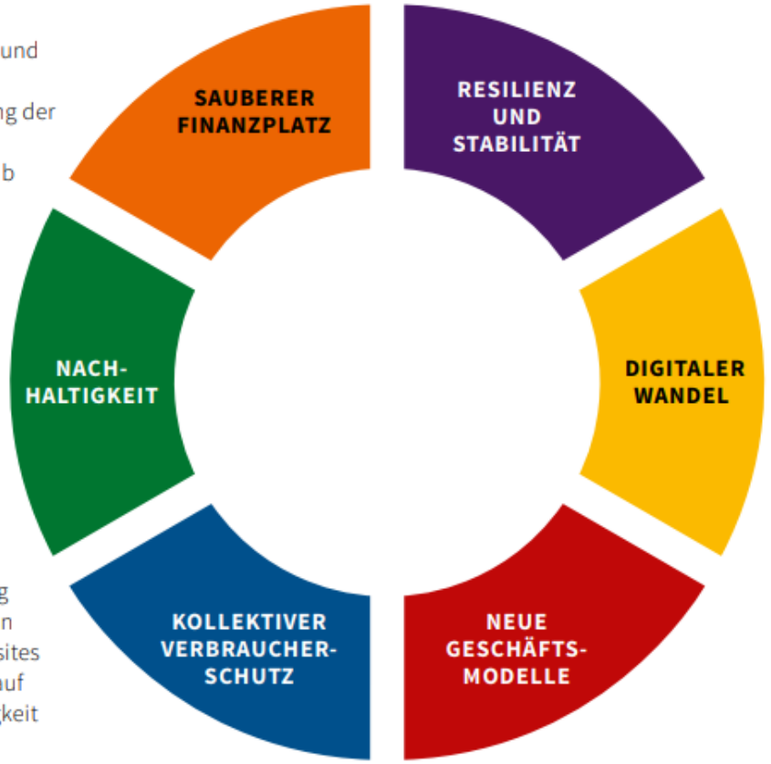
WIE WIRD IT-RISIKO BEAUFSICHTIGT?

AUFSICHTS- UND PRÜFUNGSSCHWERPUNKTE DER FMA 2023

Sauberer Finanzplatz
- Monitoring und Analyse von Trends und Geschäftspraktiken
- Automationsunterstützte Auswertung der Whistleblowing-Meldungen
- Nationaler Kompetenz- und Info-Hub für Prävention von Geldwäsche

Nachhaltigkeit
- Integration von Nachhaltigkeitsrisiken ins Risikomanagement, in die Strategie und Governance beaufsichtigter Unternehmen
- Fokus auf Offenlegung und nichtfinanzielle Berichterstattung
- Greenwashing

Kollektiver Verbraucherschutz
- Risikoorientiertes Market-Monitoring
- Transparenz bei Prämienerhöhungen
- Analyse der Informationen auf Websites
- Fokus der Verbraucherinformation auf Inflation, Altersvorsorge, Nachhaltigkeit und Krypto-Assets



Resilienz und Stabilität
- Risiken und Vulnerabilitäten identifizieren
- Kapitalausstattung verbessern, Risiken adressieren
- Nachhaltige Kreditvergabe sicherstellen
- Abwicklungsfähigkeit der Banken stärken

Digitaler Wandel
- Stabilität digitaler Systeme fördern
- Resilienz gegenüber Cyberrisiken ausbauen

Neue Geschäftsmodelle
- Regulatory Sandbox und Neukonzessionierungen
- Umsetzung IFR/IFD, „große“ Wertpapierfirmen
- Vorbereitung auf kommende europäische Regulierungen zu Kryptowerten und zur DLT-Technologie

WARUM IST DIE BEGRENZUNG VON IT-RISIKEN WICHTIG?

WARUM IST DIE BEGRENZUNG VON IT-RISIKEN WICHTIG?

„DIGITALIZATION AND IT-RISK ARE TWO SIDES OF THE SAME COIN“

Digitalisierung und Anstieg von IT-Risiken gehen Hand in Hand

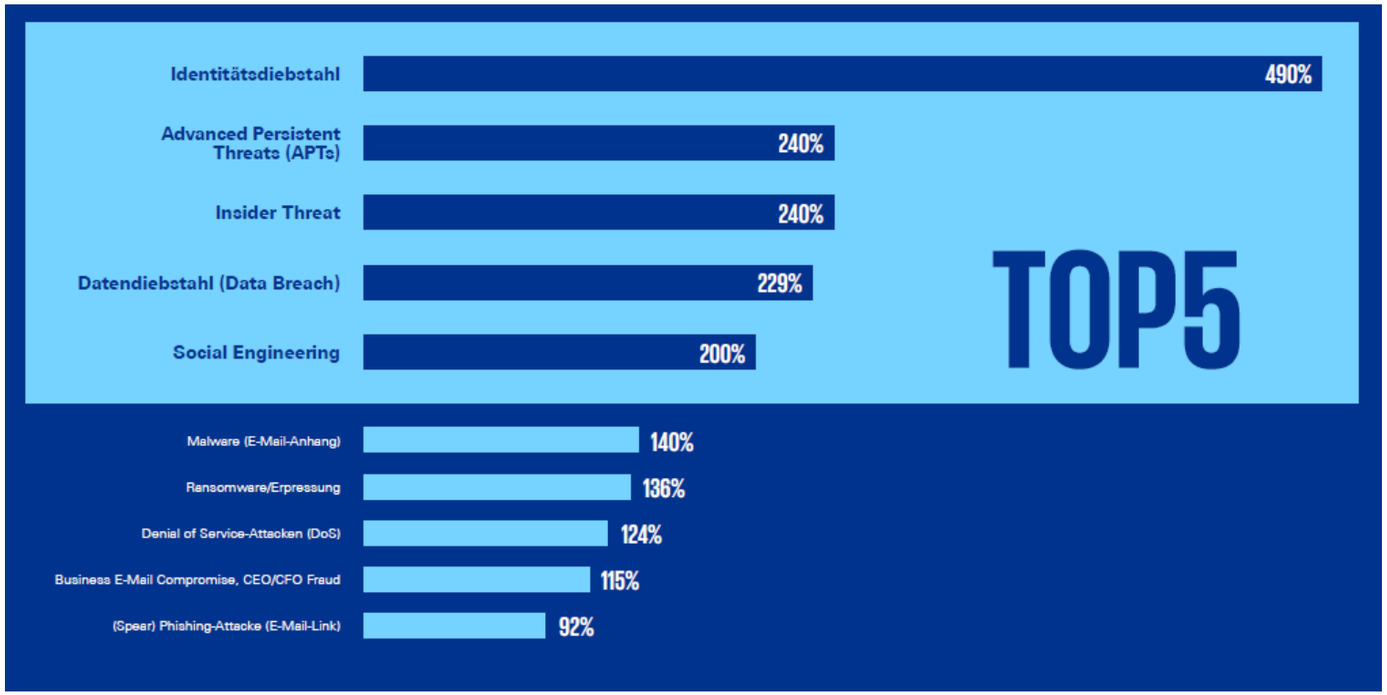
- Digitalisierung und Anstieg von IT-Risiken gehen Hand in Hand
- Finanzsektor bis 2020 TOP 1 Ziel von Cyberangriffen: seit 2021 TOP 2[1] (Top 1: Fertigungsindustrie)
- Cyber-Angriffe generell im Anstieg befindlich
- IT-Infrastruktur gewinnt ständig an Bedeutung (Digitalisierung)
- IT-Risiko laut der SSM Risk map unter den Top-3-Risiken
- nationale Schwerpunktsetzung seit 2018

[1)] IBM Security X-Force Threat Intelligence Index 2023

WARUM IST DIE BEGRENZUNG VON IT-RISIKEN WICHTIG?

CYBERSICHERHEITSLAGE IN ÖSTERREICH

Veränderungen der Angriffe von 2022 - 2023



Quelle: Bericht Cybersicherheit in Österreich 2023 (KSÖ und KPMG)

WARUM IST DIE BEGRENZUNG VON IT-RISIKEN WICHTIG?

The Lazarus heist: How North Korea almost pulled off a billion-dollar hack

21 June 2021

In 2016 North Korean hackers planned a $1bn raid on Bangladesh's national bank and came within an inch of success - it was only by a fluke that all but $81m of the transfers were halted, report Geoff White and Jean H Lee. But how did one of the world's poorest and most isolated countries train a team of elite cyber-criminals?

Quelle:
https://www.bbc.com/news/stories-57520169

WARUM IST DIE BEGRENZUNG VON IT-RISIKEN WICHTIG?

- IT-Verfügbarkeits- und Kontinuitätsrisiko
  - Ausfall von Hardware und/oder Softwarekomponenten

- IT-Sicherheitsrisiko
  - Unbefugter Zugriff auf Systeme oder Daten
  - Cyberattacken

- IT-Auslagerungsrisiko
  - Unsicheres IT-Outsourcing

- IT-Änderungsrisiko
  - Keine (zeitgerechte) und kontrollierte Steuerung von IT-Systemänderungen möglich

- IT-Datenintegritätsrisiko
  - Unvollständige, ungenaue oder inkonsistente Daten

WARUM IST DIE BEGRENZUNG VON IT-RISIKEN WICHTIG?

Millions of websites offline after fire at French cloud services firm

By Reuters, Mathieu Rosemain and Raphael Satter

3 minute read

Quelle:
https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU

WARUM IST DIE BEGRENZUNG VON IT-RISIKEN WICHTIG?

- IT-Verfügbarkeits- und Kontinuitätsrisiko
  - Ausfall von Hardware und/oder Softwarekomponenten

- IT-Sicherheitsrisiko
  - Unbefugter Zugriff auf Systeme oder Daten
  - Cyberattacken

- IT-Auslagerungsrisiko
  - Unsicheres IT-Outsourcing

- IT-Änderungsrisiko
  - Keine (zeitgerechte) und kontrollierte Steuerung von IT-Systemänderungen möglich

- IT-Datenintegritätsrisiko
  - Unvollständige, ungenaue oder inkonsistente Daten

MAßNAHMEN ZUR BEGRENZUNG VON IT- UND OPERATIONELLEN RISIKEN IM ZAHLUNGSVERKEHR

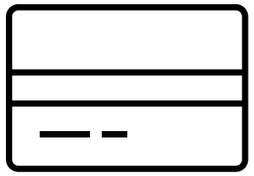
MAßNAHMEN ZUR BEGRENZUNG VON IT- UND OPERATIONELLEN RISIKEN IM ZAHLUNGSVERKEHR

WAS KANN DER ZAHLUNGSDIENSTLEISTER TUN?

- Intensivierung IT-Risikomanagement und IT-Governance
- Fokus auf Drittdienstleister-Management
- Implementierung technischer Maßnahmen zum Schutz gegen Cybervorfälle
- Aktive Beobachtung der Bedrohungslage
- Austausch und Kommunikation mit anderen Finanzmarktteilnehmern
- Awareness-Maßnahmen und Unterstützung für Zahlungsdienstnutzer:innen

MAßNAHMEN ZUR BEGRENZUNG VON IT- UND OPERATIONELLEN RISIKEN IM ZAHLUNGSVERKEHR

BEISPIEL TECHNISCHE MAßNAHME: EINFÜHRUNG DER FLÄCHENDECKENDEN STARKEN KUNDENAUTHENTIFIZIERUNG IM JAHR 2020



MAßNAHMEN ZUR BEGRENZUNG VON IT- UND OPERATIONELLEN RISIKEN IM ZAHLUNGSVERKEHR

ZWEI VON DREI ELEMENTEN AUS DER KATEGORIE WISSEN, BESITZ UND INHÄRENZ MÜSSEN ZUR AUTHENTIFIZIERUNG DES KUNDEN/DER KUNDIN HERANGEZOGEN WERDEN:

- Wissen: zB Passwort, PIN, bestimmte Wischbewegungen
- Besitz: zB mittels Kartenlesegerät eingelesene Kreditkarte/Debitkarte, App (device-binding!), Handy (SIM-Karte)
- Inhärenz: zB: Fingerabdruck, Gesichtserkennung, Spracherkennung

WANN HAT EINE STARKE KUNDENAUTHENTIFIZIERUNG ZU ERFOLGEN (§ 87 ZADIG)?

- Wenn der Zahler/die Zahlerin online auf sein/ihr Zahlungskonto zugreift
- Einen elektronischen Zahlungsvorgang auslöst (über einen Fernzugang)

DIE WICHTIGSTEN AUFSICHTLICHEN REGELUNGEN

DIE WICHTIGSTEN AUFSICHTLICHEN REGELUNGEN

EBA-LEITLINIEN UND SOFTLAW

- EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken (EBA/GL/2019/04)
  - Inhaltliche Vorgaben IT-Risikomanagement
- EBA-Outsourcing-Leitlinien (EBA/GL/2019/02)
  - Leitlinien generell zu Outsourcing; auch: IT-Auslagerungen
- EBA-Leitlinien zur Meldung von Betrugsfällen nach PSD 2(EBA/GL/2018/05)
- EBA-Leitlinien für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie (EU) 2015/2366 (PSD2) (EBA/GL/2021/03)
  - Vorgaben zur Meldung und zum Prozess
- NIS2 RL, Cyber Incident Reporting Framework
  - Vorgaben zur Meldung von Vorfällen für SI und kritische und sensible Infrastrukturen
- BCBS 239
  - Vorgaben des Basler Ausschusses für G-SIBs (global systemically important banks) und D (domestic)-SIBs

DIE WICHTIGSTEN AUFSICHTLICHEN REGELUNGEN

DORA

- Allgemeines und Zeitplan:
  - Teil des Digital Finance Package
  - Compromise Paper der portugiesischen Ratspräsidentschaft im Juni 2021
  - Trilog-Einigung Anfang Mai 2022
  - Veröffentlichung der finalen VO: Dez 2022
  - Inkrafttreten: 16.01.2023
  - Vollständiges Inkrafttreten: 24 Monate nach Inkrafttreten (2025)
  - 8 RTS, 2 ITS und 2 Leitlinien im Rahmen von DORA geplant

DIE WICHTIGSTEN AUFSICHTLICHEN REGELUNGEN

DORA

- Die wichtigsten Neuerungen
  - Fokus auf IT-Risikomanagement und Governance
  - Streamlining/Harmonisierung von Vorfallsmeldungen geplant
  - Intensivierung der Prüfungen der digitalen Betriebsstabilität im Rahmen des IKT-Risikomanagementrahmens (Stichwort: TIBER-AT)
  - Intensivierung der Steuerung des von Drittanbietern ausgehenden Risikos
  - Einführung Überwachungsrahmen für kritische IKT-Drittdienstleister
  - Förderung des Informationsaustausches (innerhalb des Finanzsektors und unter Behörden)

IT-RISIKOMANAGEMENT

Governance & Organisation		
IKT-Risikomanagement Rahmen	IKT-Systeme, -Protokolle und -Tools	Identifizierung
Schutz & Prävention	Erkennung	Reaktion & Wiederherstellung
Backup, Wiedergewinnung und Wiederherstellung	Lernprozesse und Weiterentwicklung	Kommunikation

IKT-BEZOGENE VORFÄLLE

PROZESS

- Einrichtung von Prozessen und Vorgaben zu
  - IKT-bezogenen Vorfällen
  - Überwachung, Handhabung und Weiterverfolgung von Vorfällen
  - Zuständigkeiten
  - Kommunikationspläne
  - Eskalation
  - Verfahren für Gegenmaßnahmen

IKT-BEZOGENE VORFÄLLE

KLASSIFIZIERUNG VON VORFÄLLEN

- Kriterien
  - Zahl der Betroffenen und möglicher Rufschaden
  - Dauer
  - Geografische Ausbreitung
  - Datenverlust
  - Kritikalität der betroffenen Dienste
  - Wirtschaftliche Auswirkungen (absolut und relativ)

IKT-BEZOGENE VORFÄLLE

MELDUNG

- Meldung innerhalb vorgegebener Fristen
  - Initialmeldung
  - Zwischenbericht
  - Abschlussbericht

- Gegebenenfalls erfolgt eine Weiterleitung durch Aufsichtsbehörde an ESA und NIS-Behörde und andere Stellen.
- Im Zuge von DORA Neuerungen erwartet:
  - Anpassung der Kriterien (Vereinheitlichung für alle Sektoren)
  - Meldetemplate
  - Jährlicher Bericht der ESAs zu schwerwiegenden IKT-bezogenen Vorfällen
  - Bericht über weitere mögliche Zentralisierung von IKT-Vorfallsmeldungen (EU-Meldeplattform)

PFLEGE DER KUNDENBEZIEHUNGEN MIT ZAHLUNGSDIENSTNUTZER:INNEN

ZWECK

- Bewusstseinsbildung der Kund:innen in Bezug auf sicherheitsrelevante Risiken iZm Zahlungsdiensten

MAßNAHMEN

- Prozess
- Unterstützung und Beratung im Hinblick auf neue Gefahren und Schwachstellen
- Möglichkeit zur Deaktivierung von Zahlungsfunktionen; Anpassungsmöglichkeiten bei Obergrenzen im Zahlungsverkehr
- Warnungen bei veranlassten oder fehlgeschlagenen Zahlungsversuchen
- Regelmäßige Information bei Aktualisierung der Sicherheitsverfahren

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz