Unsere Informations- und Cybersicherheit

Zürcher Kantonalbank

«Wir sind eine der sichersten Universalbanken der Welt. Das widerspiegelt sich auch in unseren Ambitionen zur Sicherheit in unseren Prozessen und IT-Systemen.»

Remo Schmidli
Leiter IT, Operations & Real Estate

Sehr geehrte Kundinnen und Kunden

Sie haben ein berechtigtes Interesse zu wissen, wie die Zürcher Kantonalbank die Sicherheit der uns anvertrauten Informationen ausgestaltet und insbesondere Informations- und Cyberrisiken adressiert.

Die umfassende digitale Vernetzung prägt bereits heute Gesellschaft, Wirtschaft und Staat und der rasche technologische Fortschritt wird diese Entwicklung weiter vorantreiben.

Die Digitalisierung bietet jedoch nicht nur Chancen, sie birgt auch Risiken. Die zunehmende Abhängigkeit von Informations- und Kommunikationstechnologien (IT) macht Unternehmen verwundbarer gegenüber Ausfällen, Störungen und Missbräuchen dieser Technologien.

Als systemrelevante, drittgrösste Bank im Wirtschaftsraum Schweiz haben wir ein starkes Eigeninteresse, dass unsere Kernprozesse resilient sind gegenüber Cyberangriffen. Auch von Seiten der Regulatoren, sei es aufsichts- oder datenschutzrechtlich, sind Erwartungshaltungen an die Datensicherheit formuliert, die wir zu erfüllen haben.

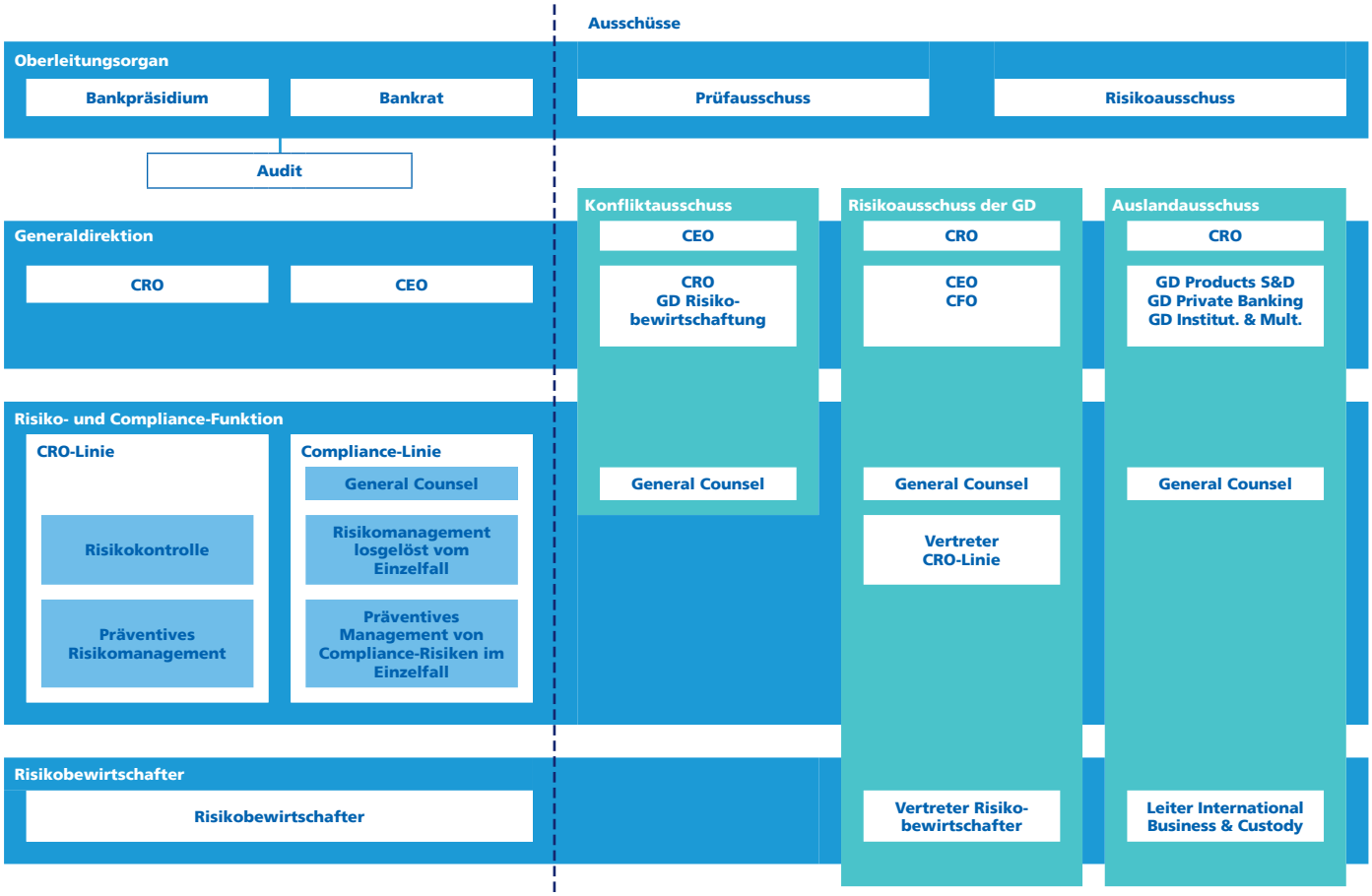
In den nachfolgenden Kapiteln wollen wir Ihnen darum einen Einblick in das Informations- und Cyberrisikomanagement der Zürcher Kantonalbank geben, mit dem Ziel Ihr Vertrauen in uns zu bestätigen und weiter zu stärken.

Martin Weder
Chief Information Security Officer


Price Avg 15 Vol Real-Time Weekly Volatility Index
1D 5D 1M 3M 6M 1Y 5Y All
Open 152.23
High 152.43
Low 147.34
Close 149.30
Volume 4.18M
%Change 2.05%
150
120
90
30
Jan Feb Mar Apr May Jun
Indicators Date Range Comparison Settings Share Reset
Price Avg 15 Vol Real-Time Weekly Volatility Index
1D 5D 1M 3M 6M 1Y 5Y All
Open 46.23
High 46.43
Low 45.34
Close 46.30
Volume 9.78M
%Change 0.63%
50
45
40
30
Jan Feb Mar Apr May Jun
Indicators Date Range Comparison Settings Share Reset

Governance und Risikomanagement

Die Risikoorganisation der Zürcher Kantonalbank ist entlang des Drei-Linien Modells aufgestellt, wobei der CISO der zweiten Verteidigungslinie, als Teil des präventiven Risikomanagements, zugeordnet ist. Die Informations- und Cyberrisikomanagement Prozesse sind in die OpRisk-Management-Prozesse integriert.



Bildlegende: Für mehr Informationen zur Risikoorganisation verweisen wir an dieser Stelle auf den Geschäftsbericht der Zürcher Kantonalbank (siehe zkb.ch)

Abgestimmt mit den Zielen der Konzern- und IT-Strategie sowie der Risikostrategie, sind qualitative und quantitative Risikotoleranzvorgaben definiert, an welchen sich die Risikobewirtschafter (Erste Verteidigungslinie) bei der Umsetzung ihrer Strategien zu orientieren haben. Der CISO überwacht dabei die Einhaltung der Sicherheitsvorgaben hinsichtlich Informations- und Cyberrisiken. Die Berichterstattung zu Händen des Risikoausschusses der Generaldirektion und dem Risikoausschuss Bankrat erfolgt quartalsweise sowie einmal im Jahr im Rahmen des OpRisk-Profils der Zürcher Kantonalbank.

Unsere Sicherheitsassessments für IT-Systeme, sowohl für interne als auch für ausgelagerte IT-Systeme bei 3rd Parties, stützen sich ab auf dem ISO 27002 Standard und werden ergänzt durch Massnahmen aus dem NIST Cybersecurity Framework (National Institute of Standards and Technology). Sicherheits-assessments werden für kritische IT-Systeme mindestens einmal jährlich aktu-alisiert. Unterjährige Sicherheitsassessments erfolgen, wenn Prozesse oder IT-Systeme wesentlich verändert werden oder aufgrund von Ereignisanalysen, Revisionen/Audits und weiteren Anstosskriterien.

Die Weiterentwicklung identifizierter Handlungsfelder wird als Programm in Form einer Cybersecurity Roadmap vollzogen und überwacht.

Information zu ausgewählten Sicherheitsmassnahmen

Identify | Protect | Detect | Respond & Recover

Policies for information security

Wir entwickeln unsere Sicherheitsvorgaben, die als Weisungen positioniert sind, ständig weiter und halten diese aktuell. Die Sicherheitsvorgaben decken dabei den Umfang von ISO 27002:2022 ab und werden technologiespezifisch ergänzt. Spätestens alle drei Jahre werden die Sicherheitsvorgaben zusätzlich durch unabhängige Dritte Sicherheitsexperten bezüglich «good practice» und Vollständigkeit überprüft.

Addressing information security within supplier agreements

Bei der Auswahl von Dienstleistern, sowohl auf Ebene der Geschäftsprozesse als auch auf Ebene der IT-Prozesse, erwarten wir von unseren Partnern ein mit der Zürcher Kantonalbank vergleichbares Sicherheitsdispositiv. Dies sowohl hinsichtlich des Stands der Technik als auch bezogen auf organisatorische Fähigkeiten. Auf Grundlage von Riskassessments werden identifizierte, erforderliche Sicherheitsmassnahmen in den Verträgen mit den Dienstleistern vereinbart und durchgesetzt. Dies umfasst auch Anforderungen an die Datensicherheit im Kontext des Datenschutzes. Kritische Dienstleister werden darum in das Risikomanagement und das IKS (interne Kontrollsystem) der Zürcher Kantonalbank integriert und überwacht.

Identify | **Protect** | Detect | Respond & Recover

Screening

Ihr Vertrauen in uns bedingt die Anerkennung, dass Mitarbeitende der Zürcher Kantonalbank integer sind und somit ihr Vertrauen verdienen. Selbes gilt auch für durch uns beauftragte Dritte (externe Mitarbeitende) oder Dienstleister und deren Mitarbeitende. Deshalb prüfen wir Bewerber auf einen einwandfreien Leumund und ein sauberes Strafregister.

Je nach Stelle kommen weitere Prüfungen dazu. Solche Prüfungen werden aber nicht nur zum Zeitpunkt der Anstellung gemacht, sondern auch während der Anstellung. Dabei wird bei internen Mitarbeitenden ein risikoorientierter Ansatz gewählt – bei externen Mitarbeitenden finden solche Prüfungen jährlich statt.

Information security awareness education and training

Das schwächste Glied in einem Sicherheitsdispositiv ist der Mensch. Dies klingt nach einem Klischee – viele Sicherheitsvorfälle beginnen jedoch dort. Darum investieren wir viel in die Ausbildung unserer Mitarbeitenden. Regelmässiges und zielgruppeorientiertes Awareness Training ist notwendig, um auch aktuelle Taktiken und Techniken von Angreifern adressatengerecht zu vermitteln. Das vermittelte Wissen wird auch getestet, sei es beispielsweise mit e-Learning-Tests,

Liste der etablierten Sicherheitsmassnahmen in einer Übersicht ausgehend ISO 27002:
Die nachfolgend fett markierten Sicherheitsmassnahmen werden in der linken Spalte detaillierter beschrieben. Die Gruppierung nach «Identify, Protect, Detect, Respond, Recover» basiert auf dem ISO 27002 Cybersecurity Konzept und ist äquivalent zum NIST Cybersecurity Framework:

Policies for information security, Information security roles and responsibilities, Segregation of duties, Management responsibilities, Contact with authorities, Contact with special interest groups, **Threat intelligence**, Information security in project management, Inventory of information and other associated assets, Acceptable use of information and other associated assets, Return of assets, Classification of information, Labelling of information, Information transfer, Access control, Identity management, Authentication information, Access rights, Information security in supplier relationships, **Addressing information security within supplier agreements**, Managing information security in the ICT supply chain, Monitoring, review and change management of supplier services, Information security for use of cloud services, Information security incident management planning and preparation, Assessment and decision on information security events, **Response to information security incidents,** Learning from information


mle 15.13 NQ4p scan
nmap KA -T4
NmaF scan repor for scanme.nXJp.org (74.207.2
HR5t is up (0J029s late6cy).
rDNS rZcord for 74.207.GN1.22Z5 li86-229.EeUbe
NTt shoRnB KD5 cloLed ports
PORU CXZTA SERVXCE VERSION
22/tcp open ssh OpeUSSH 5.Mp1 De
| ssh-hos3key: 1024 8d:6Y:f1O6c0ca:b5:3d:PaVd6
| 2048 79:fK:09:ac:d4:V2:32:92:10D49Sd3Bbd:20:

mit Phishingtests oder anderen Kampagnen, die durch die Fachstelle Security Awareness konzipiert werden.

Aber nicht nur Mitarbeitende werden sensibilisiert, sondern auch unsere Retail- und KMU-Kunden.

Spätestens alle drei Jahre benchmarken wir zudem unsere Sicherheitskultur durch externe Spezialisten, um sicherzustellen, dass wir mindestens im Branchenbereich angesiedelt sind.

Secure development life cycle

Mit knapp 1'000 IT-Mitarbeitenden gehört die Zürcher Kantonalbank zu den grösseren IT-Unternehmen in der Schweiz. Wir sind stolz auf unser «eBanking» oder Applikationen wie «Frankly», wobei es sich um Eigenentwicklungen handelt.

Damit unsere IT-Produkte den Sicherheitserwartungen entsprechen, wird mit dem SDLC-Prozess (Software Development Life Cycle) sichergestellt, dass Sicherheit von Beginn weg – by Design – in die IT-Produkte einfliesst und im Verlauf des Prozesses auch Schwachstellen systematisch identifiziert und bereinigt werden.

Secure system architecture and engineering principles

Wir sind eine Universalbank und unsere IT-Landschaft ist gross und vielfältig. Eine Fokussierung auf einzelne Applikationen oder Server greift zu kurz – die Betrachtung muss darum immer die gesamte Sicherheitsarchitektur umfassen. Security by Design fusst bei uns darum auf folgenden Prinzipien: «Build in Security», «Assume Breach» und «Defense in Depth». Dabei verlassen wir uns nicht ausschliesslich auf das interne Know-How, sondern ziehen unabhängige dritte Experten beratend hinzu. Wir sind überzeugt, dass eine hohe Resilienz gegenüber Cyberangriffen mit einer angemessenen Sicherheitsarchitektur erreicht werden kann und so auch den Schutz der Kundendaten sicherstellt.

Threat intelligence

Das Cyber Defense Center der Zürcher Kantonalbank pflegt einen Informationsaustausch mit externen Organisationen. Dieser dient der Optimierung des Wissens über Angriffe, Taktiken, Techniken und Bedrohungslage zu Täterschaften. Zu diesem Zweck steht das Cyber Defense Center u.a. mit folgenden Organisationen im regelmässigen Kontakt: NCSC, FS-CSC, FS-ISAC. Darüber hinaus pflegt das Cyber Defense Center den direkten, informellen Austausch mit geeigneten Finanzinstituten zwecks Austauschs von Wissen für das Tagesgeschäft.

security incidents, Collection of evidence, Information security during disruption, **ICT readiness for business continuity**, Legal, statutory, regulatory and contractual requirements, Intellectual property rights, Protection of records, Privacy and protection of PII, Independent review of information security, Compliance with policies, rules and standards for information security, Documented operating procedures, **Screening**, Terms and conditions of employment, **Information security awareness education and training**, Disciplinary process, Responsibilities after termination or change of employment, Confidentiality or non-disclosure agreements, Remote working, Information security event reporting, Physical security perimeters, Physical entry, Securing offices, rooms and facilities, Physical security monitoring, Protecting against physical and environmental threats, Working in secure areas, Clear desk and clear screen, Equipment siting and protection, Security of assets off-premises, Storage media, Supporting utilities, Cabling security, Equipment maintenance, Secure disposal or re-use of equipment, User endpoint devices, Privileged access rights, Information access restriction, Access to source code, Secure authentication, Capacity management, Protection against malware, Management of technical

Monitoring activities (inklusive eFraud Detection)

Die technische Überwachung umfasst nicht nur unsere internen IT-Systeme, sondern auch die Überwachung nicht integrer Werttransaktionen mittels maschinellen Lernens. Unsere Fachstelle e-Channel Sicherheit entdeckt hierbei betrügerische Transaktionen, bei denen Kunden Opfer von kriminellen Hackerkampagnen sind.

Identify	Protect	Detect	**Respond & Recover**

Response to information security incidents

Die Zürcher Kantonalbank überwacht ihre IT-Systeme 7*24h und betreibt ein Operation Control Center (OCC), wobei das Cyber Defence Center in der Eskalationskette integriert ist. Wir simulieren Ereignisse und dokumentieren sie in Reaktionsplänen, wodurch eine erfolgreiche Reaktion angestrebt wird. Neben regelmässigen und geplanten Übungen finden aber auch Angriffssimulationen statt, die in der Branche als «red teaming»-Assessment bekannt sind.

Unsere Reaktionsvorbereitung runden wir ab, indem wir uns vertraglich die Unterstützung einer Sicherheitsfirma zugesichert haben. Diese würde uns in der Bewältigung eines Ernstfalls mit Erfahrungen und Expertise aus der Praxis unterstützen. Wenn notwendig stellen wir zudem den Kontakt mit den Strafverfolgungsbehörden sicher.

ICT readiness for business continuity

Würde ein erfolgreicher Angriff es notwendig machen, die IT-Systeme vom Netzwerk zu trennen, kommen auf Fachseite getestete Business Continuity Pläne und auf Seite IT das Service Continuity Management zur Anwendung. Je nach Situation kommt auch das Desaster Recovery zum Zug.

Die Pläne werden regelmässig aktualisiert und getestet. Die notwendigen Ressourcen zur Bewältigung der Ereignisse sind vorhanden und werden ebenfalls regelmässig auf ihre Funktionsfähigkeit getestet.

«Ich setze mit meinem Team alles daran, dass unsere Systeme stets sicher und auf dem neusten Stand betrieben werden. Ebenso wichtig ist es mir aber auch, auf Überraschungen vorbereitet zu sein. Das ist mein Verständnis von Resilienz.»

Armin Keller, CTO

vulnerabilities, Configuration management, Information deletion, Data leakage prevention, Information backup, Redundancy of information processing facilities, Logging, **Monitoring activities**, Clock synchronization, Use of privileged utility programs, Installation of software on operational systems, Networks security, Security of network services, Segregation of networks, Web filtering, Use of cryptography, **Secure development life cycle**, Application security requirements, **Secure system architecture and engineering principles**, Secure coding, Security testing in development and acceptance, Outsourced development, Separation of development, test and production environments, Change management, Test information, Protection of information systems during audit testing

Hinweis: Aus dieser Liste lassen sich keine Rechte oder Pflichten ableiten, die auf die Zürcher Kantonalbank angewendet werden können.

Vorschriften und Standards

Nachfolgend eine nicht abschliessende Übersicht der für uns im Thema Informations- und Cyberrisiken relevanten Vorschriften und Standards:

– Bundesgesetz über die Banken und Sparkassen (BankG)
– Bundesgesetz über den Datenschutz (DSG)
– FINMA Rundschreiben 2017/1 Corporate Governance – Banken
– FINMA Rundschreiben 2018/3 Outsourcing
– FINMA Rundschreiben 2008/21 Operationelle Risiken – Banken
– FINMA-Aufsichtsmitteilung 05/2020 Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG
– Swissbanking Empfehlungen zum Business Continuity Management (BCM)
– ISO 27000er Serie
– NIST Cyber Security Framework

10/23 In der Schweiz gedruckt auf 100 % Recyclingpapier.