Bild: Shutterstock

Cyber-Angriff auf Banken

Welche Vorkehrungen werden getroffen – wie ist in der Krise zu kommunizieren?

Dieter Oberli, Leiter Fachstelle Business Continuity Management

Luzern, 24. Oktober 2017

RAIFFEISEN

Schlüsselzahlen

3,7 Mio. Kundinnen und Kunden

255 Raiffeisen-banken

1,9 Mio. Mitglieder

930 Standorte

10‘986 Mitarbeitende

Aa2 Rating

RAIFFEISEN

Aufgabenteilung
Raiffeisen Schweiz – Raiffeisenbanken

Raiffeisen Schweiz

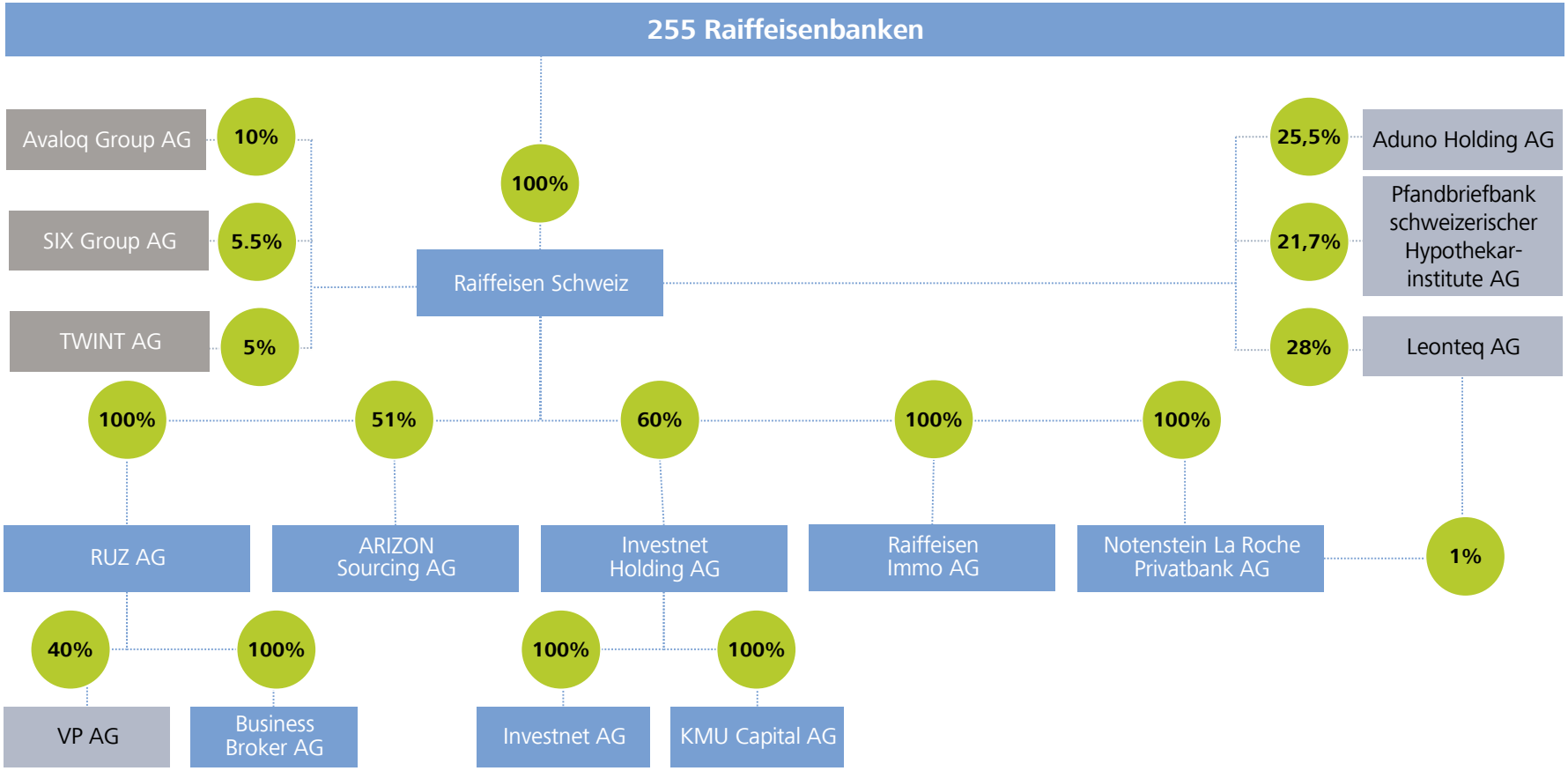
- Strategische Führung
- Schaffen von Rahmenbedingungen
- Zentralbank
- Risikomanagement
- Vertretung von Interessen

Raiffeisenbanken

- Markt- und Unternehmensverantwortung
- Erbringung bedürfnisgerechter Bankdienstleistungen

RAIFFEISEN

Strategische Kooperationen und wesentliche Beteiligungen, Stand 15.09.2017



Im Konsolidierungskreis

Nach Equity-Methode bewertete Beteiligungen

Strategische Kooperation

RAIFFEISEN

Wieviel Sicherheit ist genügend?

Ist der Wettlauf gegen Hacker zu gewinnen?

Die individuelle Ausgestaltung der Sicherheitsmassnahmen ist von Branche zu Branche verschieden – jedoch darf davon ausgegangen werden, dass sich die Banken im oberen Bereich der möglichen Vorkehrungen bewegen.

Obwohl scheinbar Finanzinstitute ein begehrtes Ziel von Attacken aus dem Cyberspace abgeben, haben letzthin verschiedene Meldungen das ganze Spektrum betroffener Geschäfts- und Lebensbereiche aufgezeigt.

Mittlerweilen dürfte überall angekommen sein, dass das Sankt-Florian-Prinzip keine geeignete Verhaltensweise ist, potentielle Bedrohungen oder Gefahrenlagen nicht zu lösen.

RAIFFEISEN

Das Vertrauen in die Banken ist so hoch wie noch nie

Und somit auch höher als vor der Finanzkrise

Ergebnis einer repräsentativen Umfrage im Auftrag der Schweizerischen Bankiervereinigung SwissBanking Januar 2017

- 85 Prozent der Schweizerinnen und Schweizer stellen ihrer Bank gute bis sehr gute Noten aus
- 95 Prozent der befragten Personen halten ihre Bank für vertrauenswürdig

ABER:

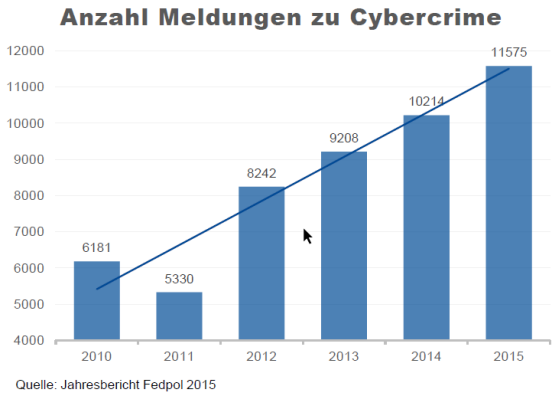
- 86 Prozent betrachten die Risiken durch kriminelle Informatikattacken als gross oder sehr gross

RAIFFEISEN

Sind diese Befürchtungen berechtigt?
Oder ist alles nur Angstmacherei?

Resultat einer Umfrage der KPMG bei Schweizer Unternehmen (2016):

- 54 Prozent der befragten Unternehmen wurden bereits **Opfer** von Cyberattacken
- Bei 44 Prozent der betroffenen Betriebe sorgten diese Angriffe für **gravierende Störung** der Geschäftsprozesse
- Über 25 Prozent der betroffenen Betriebe befürchten, einen bleibenden **Reputations-schaden** davongetragen zu haben



Quelle: Jahresbericht Fedpol 2015

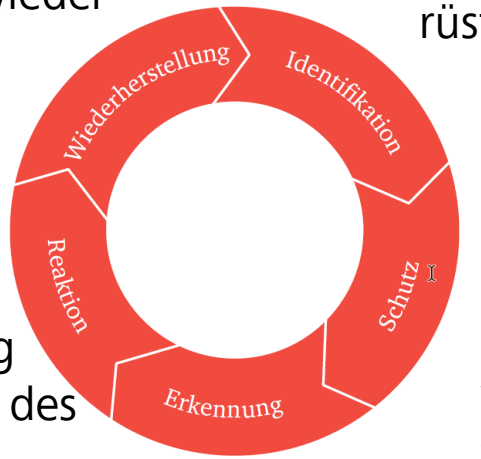
Quelle: KPMG-Bericht 'Internet of Things increases the risk of cybercrime in Switzerland' 2016

Die Erwartungen/Vorgaben der FINMA

neue Bestimmungen per 1. Juli 2017

Banken müssen die erforderlichen Massnahmen definieren, um zu garantieren, dass die Verfügbarkeit und Integrität der Systeme sowie korrumpierte oder verloren gegangene Daten nach einer Cyberattacke wiederhergestellt werden können.

Banken müssen Abhilfemassnahmen identifizieren, bewerten und planen, um sich für die Bewältigung von Cybervorfällen zu rüsten.



Banken müssen die Prozesse, Personen und Instrumente definieren, die für die Reaktion auf eine Cyberattacke notwendig sind, insbesondere zur Wahrung des normalen Geschäftsbetriebs.

Banken müssen Massnahmen ergreifen, die die unbefugte Extraktion von Daten ausserhalb des Finanzinstituts verhindern, indem die Datenflüsse überwacht werden.

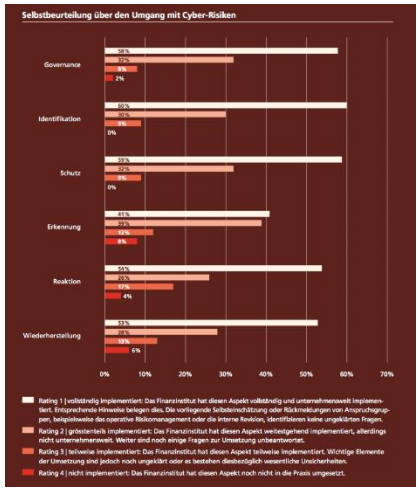
Banken müssen ihre Überwachungsansätze verbessern, die es ihnen ermöglichen, jegliches unbefugte Eindringen in ihr internes Netzwerk zu blockieren, Unregelmässigkeiten bei den Datenflüssen innerhalb des Netzwerks zu erkennen und effektiv mit Sicherheitswarnungen umzugehen.

RAIFFEISEN

Wie war der Stand der Vorbereitungen?

FINMA ortete noch grössere Lücken

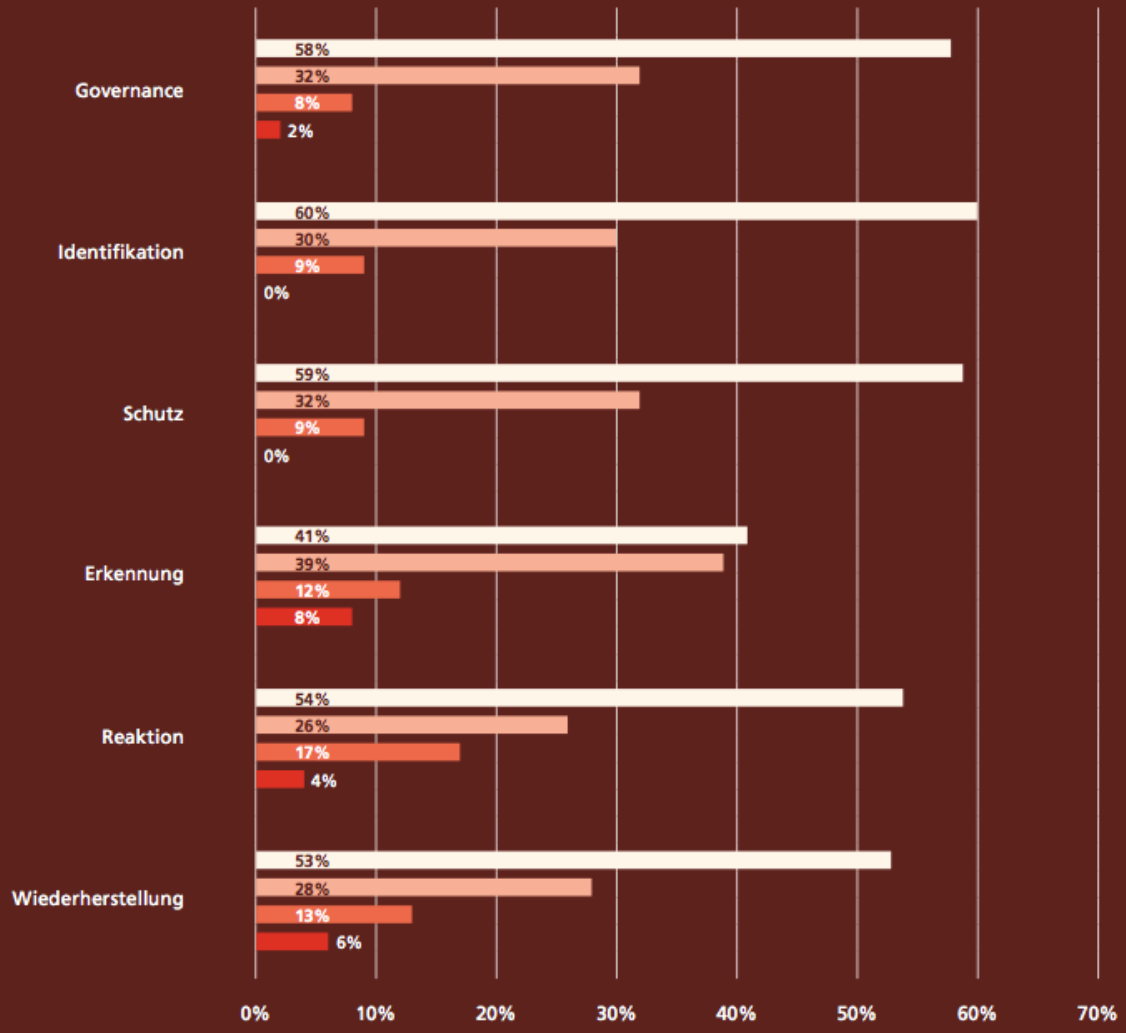
Kein besonders beruhigendes Bild vermittelte eine durch die FINMA beauftragte Selbstdeklaration bei den Kategorie-3-Banken im November 2105, die mit ihrem Gewicht ein «bedeutendes Risiko» für das Schweizer Finanzsystem darstellen.



Die FINMA lässt die Umsetzung ihrer Vorgaben durch externe Audits überprüfen.

RAIFFEISEN

Selbstbeurteilung über den Umgang mit Cyber-Risiken



Rating 1 | vollständig implementiert: Das Finanzinstitut hat diesen Aspekt vollständig und unternehmensweit implementiert. Entsprechende Hinweise belegen dies. Die vorliegende Selbsteinschätzung oder Rückmeldungen von Anspruchsgruppen, beispielsweise das operative Risikomanagement oder die interne Revision, identifizieren keine ungeklärten Fragen.

Rating 2 | grösstenteils implementiert: Das Finanzinstitut hat diesen Aspekt weitestgehend implementiert, allerdings nicht unternehmensweit. Weiter sind noch einige Fragen zur Umsetzung unbeantwortet.

Rating 3 | teilweise implementiert: Das Finanzinstitut hat diesen Aspekt teilweise implementiert. Wichtige Elemente der Umsetzung sind jedoch noch ungeklärt oder es bestehen diesbezüglich wesentliche Unsicherheiten.

Rating 4 | nicht implementiert: Das Finanzinstitut hat diesen Aspekt noch nicht in die Praxis umgesetzt.

Quelle: FINMA

RAIFFEISEN

Wie unterscheidet sich eine ‘Cyber-Attacke’ von einer ‘normalen’ Krise?

Vorab: Jede Krise ist per Definition ein aussergewöhnliches Ereignis, welches mit der ordentlichen Organisation nicht (oder nicht zeitgerecht) bewältigt werden kann.

Die Besonderheit der Cyberkriminalität besteht darin, dass ein **unbekannter Akteur** ins Spiel kommt und nahezu von jedem Ort der Welt aus agieren und seine Spuren relativ gut verschleiern kann.

Bild Shutterstock

Im Gegensatz zur greifbaren Krise ist eine Cyber-Attacke **nicht sofort** mit dem gesunden Menschenverstand **einschätzbar**.

Eine Cyber-Attacke muss **nicht unmittelbar** erkannt werden, der Angriff kann schon vor Wochen begonnen haben.

Eine negative Publizität mit abwertenden Kommentierungen, Spekulationen über Hergang und Täter sowie ein fortschreitender **Vertrauensverlust** seitens Kunden wird schneller eintreten.

RAIFFEISEN

Massnahmen zur Identifikation und Schutz vor Cyber-Attacken

Die wichtigste Massnahme war, ein Verständnis dafür zu bilden, welche Daten in unserem Unternehmen vorhanden, in welchem Masse diese angreifbar und schützenswert sind.

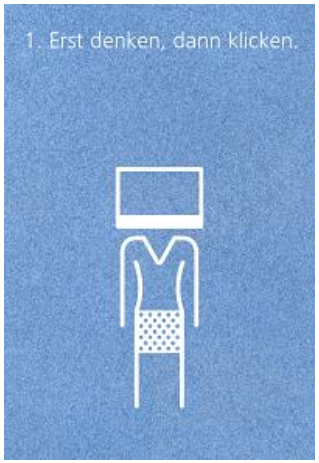
Erst dadurch war es möglich, dedizierte Massnahmen zur Bewältigung von Sicherheits-Vorfällen vollständig zu etablieren.

Die Analyse umfasst ebenfalls Daten, welche an externe Partner übermittelt und durch diese mit demselben Schutzbedarf behandelt werden müssen. Im Rahmen einer Due-Diligence-Bewertungen werden die Drittparteien hinsichtlich des Managements des Cyberrisikos bewertet und müssen ggf. zusätzliche Massnahmen ergreifen.

Für effektive, zentralisierte Sicherheitswarnungen zu garantieren, haben wir ein Security Operations Center, SOC in der IT-Organisation etabliert.

Massnahmen zur Erkennung von Cyber-Attacken

Neben technischen Massnahmen hat immer noch der Mensch das grösste Potenzial, Unregelmässigkeiten zu verhindern resp. zu erkennen.



Dazu hat Raiffeisen eLearning-Programme entwickelt (Pflicht-Kurse) und informiert regelmässig die Mitarbeitenden zu diem Thema (Schaffen von Awareness).

RAIFFEISEN

Massnahmen zur Reaktion auf Cyber-Attacken

Das Chaos entsteht nicht durch den gemachten Fehler, sondern durch die Art und Weise, wie nachher damit umgegangen wird.

Die vorbereiteten Massnahmen aus dem BCM helfen dabei, sich sicher durch die Krise zu bewegen.

Vorbereitete Massnahmen zur externen Krisenkommunikation

Medienmitteilung
Medienkonferenz
Q&A, Sprachregelungen
Internet / Website
Call Center
Hotline
E-Banking Meldungen
Monitoring
Abstimmung interne Kommunikation

Jeweils mit Ansprechpartner, Schnittstellen, Vorgehen, Hilfsmittel, etc.

RAIFFEISEN

Massnahmen zur Wiederherstellung nach Cyber-Attacken

Auch hier gilt zu berücksichtigen, was im Rahmen der Vorsorge für das IT resp. Business Continuity Management vorbereitet wurde.

Falls die Glaubwürdigkeit durch den Vorfall gelitten hat, kann eine gute Krisen-Kommunikation unterstützen, diese rascher wiederherzustellen.

Nicht zu vergessen sind, Massnahmen zur Verbesserung des Konzepts abzuleiten (Lessons Learned).

RAIFFEISEN

Grundsätze der Krisenkommunikation

Kennen wir doch alle …
Keine Angst- oder Panikmacherei betreiben.
Trotzdem: Die Stärke des Krisenmanagements und der Krisenkommunikation sind das Resultat der (strategischen) Vorarbeiten. Deshalb: Bereits vor der Krise agieren, statt nur in der Krise zu reagieren.

Machen wir doch immer so …
Rückblick (was ist passiert?)
Überblick (wie gehen wir damit um?)
Ausblick (was werden wir tun und wann gibt es neue Erkenntnisse?)

Dies sollte auch bei einer Cyber-Attacke nicht anders sein!

RAIFFEISEN

Empfehlungen zur Krisenkommunikation

Lernen von den andern

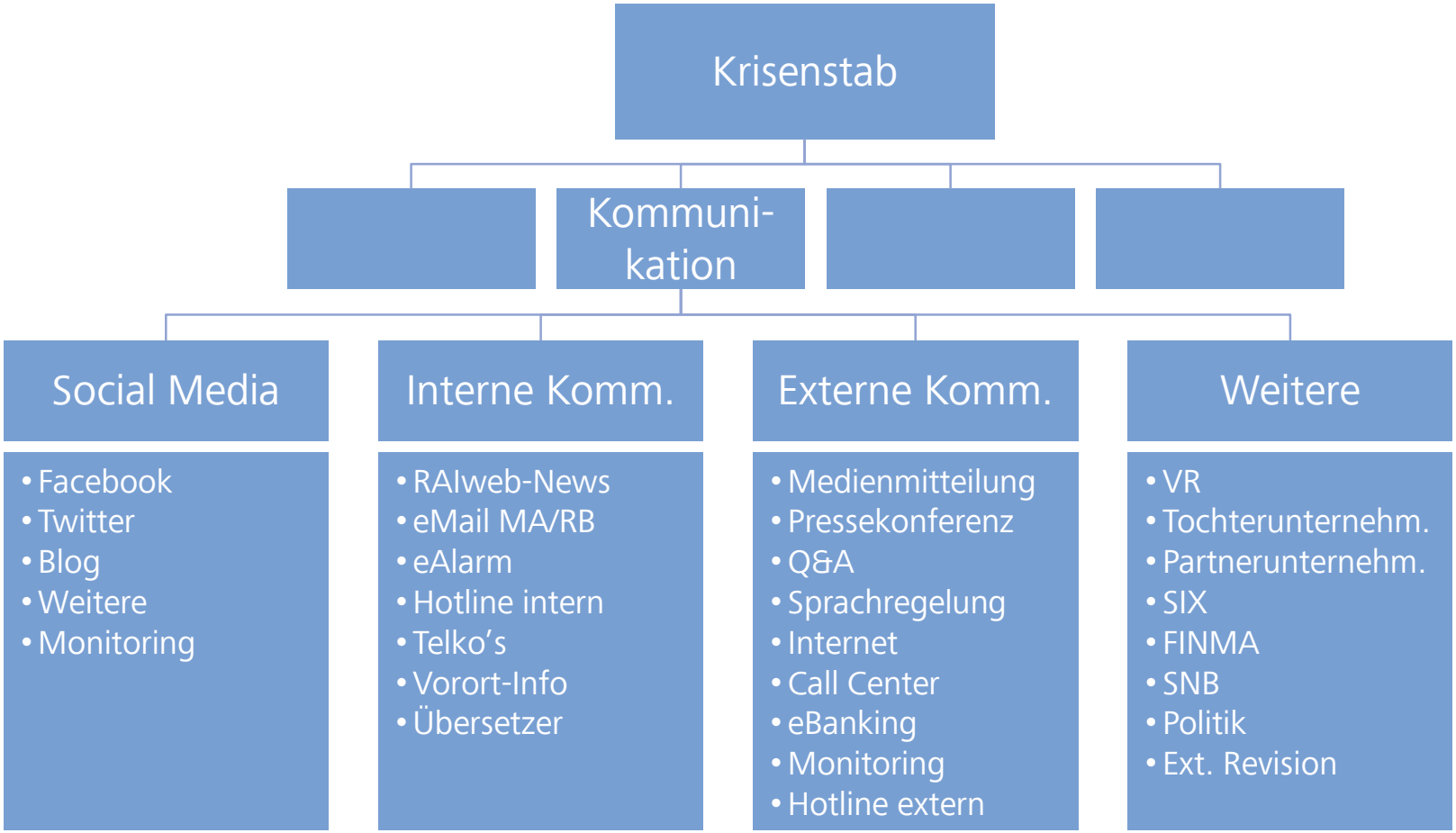
Google liefert auf das Stichwort Krisenkommunikation über 350’000 Treffer.

‘gelungene krisenkommunikation beispiel’ liefert 200’000,
‘schlechte krisenkommunikation beispiel’ immerhin 159’000

Was andere gut machen, sollte man versuchen zu adaptieren. Was negativ beurteilt wird, dient zur Selbstreflexion.

RAIFFEISEN

Praxisbeispiel Funktionen Krisenkommunikation



RAIFFEISEN

Besten Dank für Ihre Aufmerksamkeit

Niemand wünscht sich eine Krise um besser zu werden. Aber wenn man schon eine ernsthafte Krise am Hals hat, sollte man sie wenigstens nutzen.

RAIFFEISEN