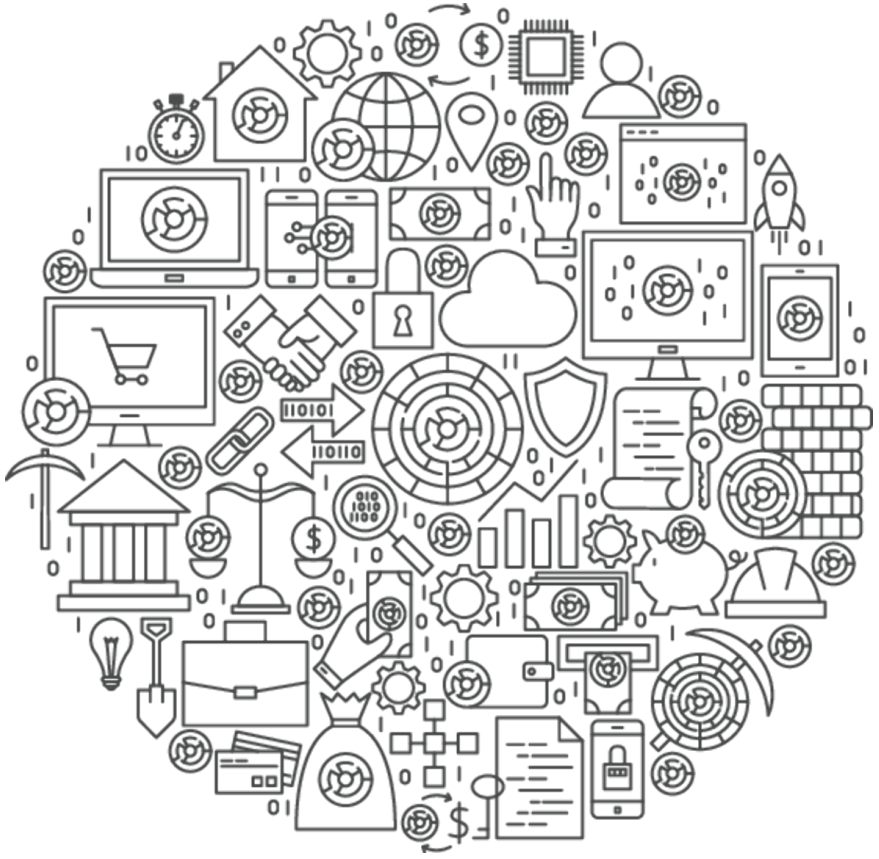
Deloitte.



Cyber-Security

# Cyber Resilienz 2022 in der Finanzbranche

Reto Häni| 17. Mai 2022

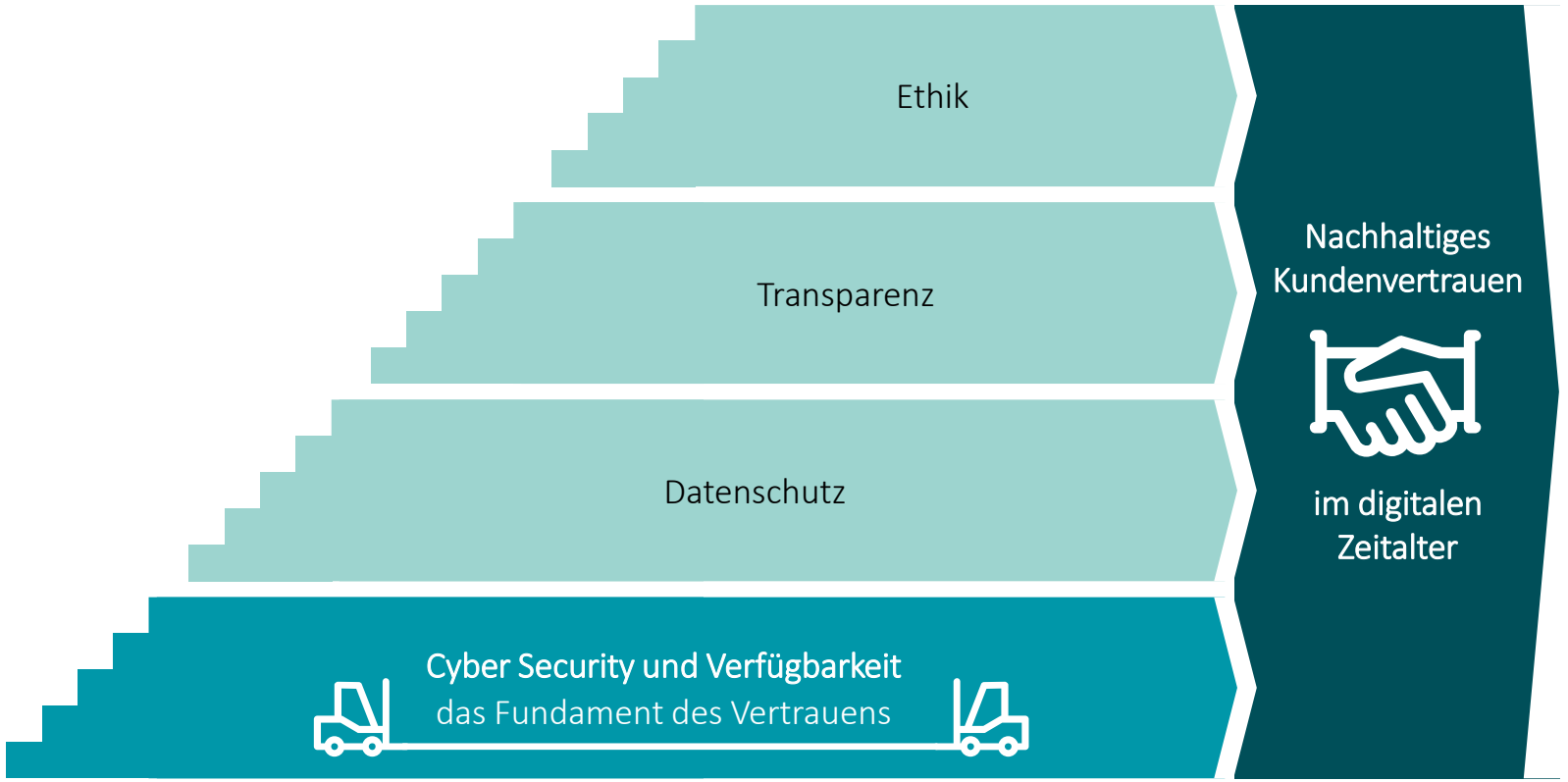
# Agenda

- Nachhaltiges Kundenvertrauen im digitalen Zeitalter
- Cyber-relevante Herausforderungen im digitalen Zeitalter
- Zentrale Fragen, die sich Banken stellen müssen
- Wichtige Themen, die Banken aktuell angehen
  - Reduktion der Angriffsfläche
  - Erhöhung der Resilienz
  - Sicherheit in agiler Umgebung
- Der Beitrag vom Business
- Konklusion, *Diskussion und Fragerunde*

# Nachhaltiges Kundenvertrauen im digitalen Zeitalter

Cyber-Security bildet das Fundament eines nachhaltigen Vertrauensverhältnis zwischen Kunden und Bank. Vorfälle bleiben auch in Zukunft unausweichlich, aber deren Schadensausmass können Banken grösstenteils direkt kontrollieren.

## Der Weg zum Vertrauen – mehr als nur ein Versprechen

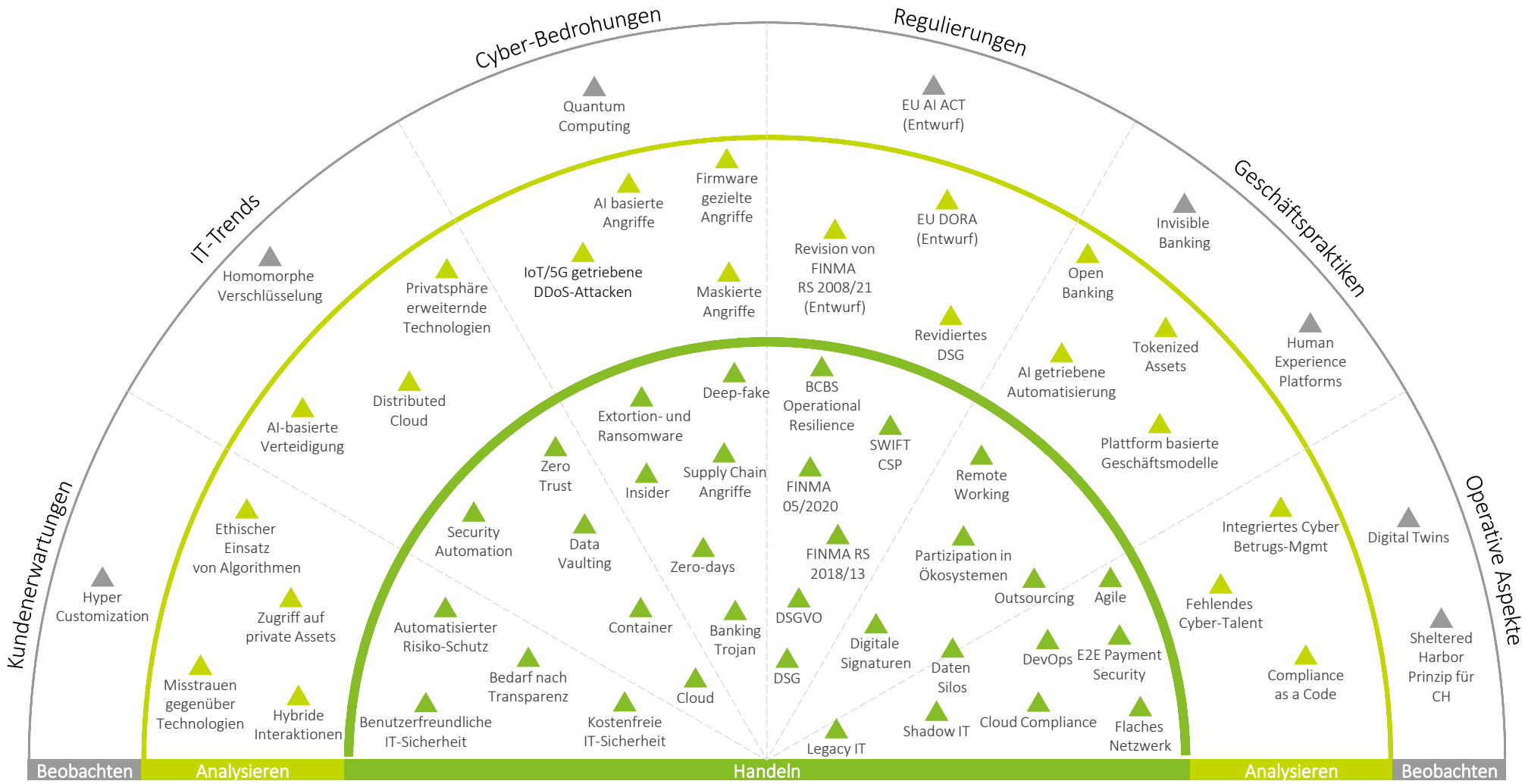



## Chance für Schweizer Banken

- Schweizer Banken können auf einer starken Reputation ihrer Sicherheit und Diskretion aufbauen und geniessen somit einen Vertrauensvorsprung
- Erfahrungsschatz im Bereich Sicherheit und Betrugsbekämpfung ist eine klare Differenzierung zu «New Entrants»
- Banken können den Lead bei der Gestaltung einer sichereren Gesellschaft übernehmen und als Meinungsmacher agieren

# Cyber-relevante Herausforderungen im digitalen Zeitalter

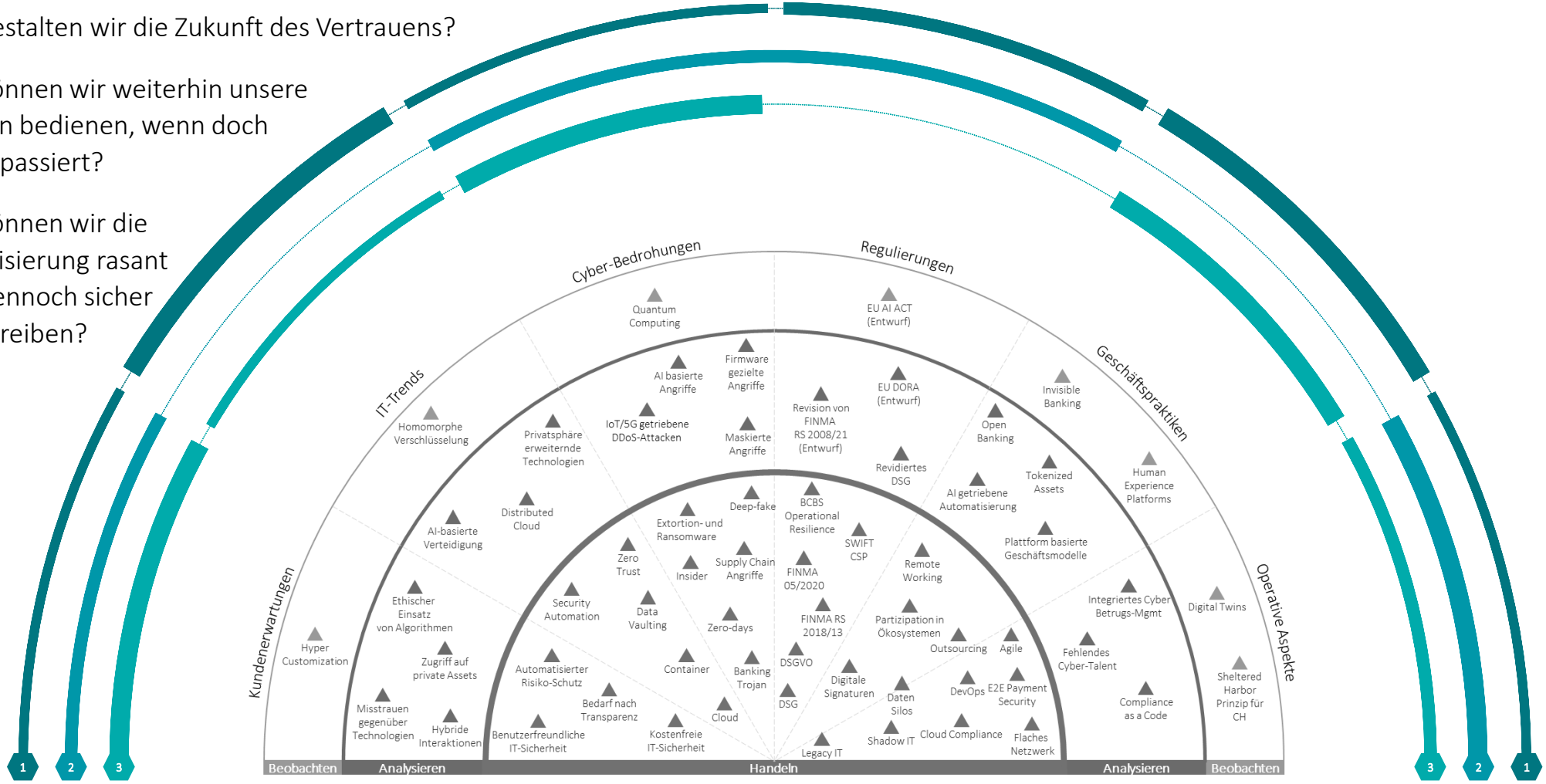
Neben anspruchsvollen Cyber-Bedrohungen gibt es unzählige Themen, welche die Sicherheit einer Bank beeinflussen. Sich auf die wichtigsten Themen zu fokussieren bleibt bei dieser Vielfalt eine wesentliche Herausforderung für jede Bank.



# Zentrale Fragen, die sich Banken stellen müssen

Trotz der Vielfalt von Themen, welche Banken im Rahmen ihrer Cyber-Sicherheitsstrategie berücksichtigen müssen, gibt es aus Kundensicht drei zentrale Fragen, die sich jede Schweizer Bank stellen muss.

1. Wie gestalten wir die Zukunft des Vertrauens?
2. Wie können wir weiterhin unsere Kunden bedienen, wenn doch etwas passiert?
3. Wie können wir die Digitalisierung rasant und dennoch sicher vorantreiben?



# Wichtige Cyber-Themen, die Banken aktuell angehen

Ein Umdenken ist gefordert. Banken müssen weiterhin signifikant in die Weiterentwicklung ihrer Sicherheitsmassnahmen investieren, zeitgleich aber auch sicherstellen, dass Cyber-Security nicht Innovationen verlangsamt oder gar verhindert.

Sicherheit in agiler Umgebung

Reduktion der Angriffsfläche

Erhöhung der Resilienz

# Adoption agiler Sicherheit

Innovation im digitalen Zeitalter bedingt eine business-orientierte, anpassungsfähige und effiziente Cyber-Security, gekennzeichnet durch einen hohen Grad an Automatisierung, Standardisierung und Zusammenarbeit.

## Handlungsbedarf

Compliance-Ära | Risk-Ära

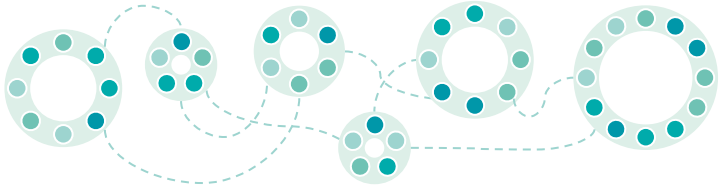
1995 2010

Der richtige Einsatz von Cloud kann Entwicklungszyklen signifikant verkürzen.

## Lösungsansätze

**Ära der Reife und Ubiquität**

2020+ Agile, adaptierbare und integrierte Cyber Security Organisation



**Beschleunigte Entwicklungszyklen**

Pipelines optimiert für Sicherheit und Geschwindigkeit

Schnelles und sicheres Entwickler-Onboarding

Wochen → GO LIVE

Kontinuierliche Compliance der Applikationen/Systeme

**Beschleunigte Entwicklung**

- Dyn. aktualisierte Open Source Lib.
- Verwaltung von Schlüssel und Zert.
- Vorlagen und Goldene Images
- Gehärtete Container Images

**Schnelle Fehlerbehebung**

- ChatOps zw. Sec, Dev und SRE Teams
- App. Monitoring/ Beobachtung
- Tracing von verteilten APIs
- Proaktive Resilienz-Tests der Systeme

**Lightweight Security-Tooling**

- API Security
- Statische Analysen
- Entwickler-freundlich
- Open Source Tooling

## Chancen

- Signifikante Beschleunigung der Entwicklungszyklen auf hohem Qualitäts-/Sicherheitsstandard
- Wertschätzung vom Business und somit höhere Compliance bzgl. Einhaltung von Vorgaben
- Steigerung der Job-Attraktivität für Cyber-Security-Fachkräfte und somit niedrige Fluktuation
- Erhöhte Kosteneffizienz erlaubt Budgetumverteilung zu anderen wichtigen Cyber-Themen

# Reduktion der Angriffsfläche

Anspruchsvolle Cyberangriffe und Veränderungen der Unternehmensumgebung haben den traditionellen «Burg-und-Wassergraben»-Sicherheitsansatz untergraben – Neu gilt: Niemals vertrauen, immer überprüfen.

## Handlungsbedarf

Mit einem traditionellen Sicherheits-ansatz kann eine einzige Schwach-stelle zu einem Flächenbrand führen

## Zero Trust als möglicher Lösungsansatz

| Vom traditionellen Ansatz | … zu Zero Trust |
|---|---|
| Netzwerk und Perimeter | **Ressourcen, nicht Netzwerke** |
| Implizites Vertrauen der internen Kommunikation | **Jede Kommunikation ist gesichert** |
| Vorausbestimmter statischer Zugriff | **Dynamischer Zugriff pro Sitzung** |
| Statisches Vertrauen basiert auf Benutzeranmeldedaten | **Zugriff bestimmt durch dynamische Richtlinien** |
| Vertrauen im eigenen Netzwerk wird vorausgesetzt | **Keinem Asset wird standardmässig vertraut** |
| Teilweise automatisierte aber lückenhafte Überwachung | **Kontinuierliche Überwachung und Auswertung** |
| Statische Authentisierung im internen Netzwerk | **Dynamische Authentisierung und Autorisierung** |

## Chancen

- Ermöglichung des „modernen Arbeitsplatz“ mit stets sicherem und flexiblem Zugang
- Schnellere und sicherere Innovation durch nahtlose Integration von Ökosystemen
- Reduzierung der Sicherheits-kosten durch Minimierung der IT-Komplexität
- Genauere Echtzeiterkennung und kontinuierliche Überwachung von Risiken
- Begrenzung der Auswirkung / Explosionsradius von Cyber-Vorfällen

# Erhöhung der Resilienz

Gross angelegte destruktive Cyber-Attacken haben gezeigt, dass klassische Ansätze für IT Disaster Recovery und Business Continuity nicht mehr ausreichen. Eine viel umfangreichere Vorbereitung ist zwingend.

## Handlungsbedarf

Alle haben einen Plan,
bis sie getroffen werden

Die Wiederherstellung der Business Services und der darunterliegenden Infrastruktur kann Wochen dauern, wenn ungenügend vorbereitet

## Prioritäten zur Erhöhung der Resilienz

- **Organisatorische Ausrichtung und Bereitschaft**
- **Priorisierte End-to-End Wiederherstellung der Business Services**
- **Umfangreicher Baukasten für Wiederherstellung**
- **Maximierte Leistungsfähigkeit und Kapazität**
- **Effektive interne und externe Kommunikation**

## Chancen

- Beschleunigte Wiederherstellung der Geschäftstätigkeiten – in Tagen statt Wochen
- Umfangreiches Verständnis der Wertschöpfungskette und die damit verbundenen Risiken
- Neuausrichtung des Business Continuity Management auf aktuelle Bedrohungen
- Automatiseirte Orchestrierung von gesamten Wiederherstellungssequenzen

# Beitrag vom Business

Cyber Security ist nicht nur ein Business Risiko, sondern eine Notwendigkeit, um erfolgreich zu operieren und Geschäfte zu tätigen. Dies impliziert, dass das Business neben der IT einen wesentlichen Beitrag zu Cyber Security zu leisten hat.

Sicherheit in agiler Umgebung

Reduktion der Angriffsfläche

Erhöhung der Resilienz

## Beitrag vom Business

- Simplifizierung der Applikations- und Systemlandschaft – die Basis zur Reduktion der Angriffsfläche
- Reifer Produktlebenszyklus, der auch zugrunde liegende Anwendungen abdeckt (inkl. Decommissioning)
- Klare Strategie zur Adoption von Cloud-basierten Technologien

- Festlegung der Wiederherstellungssequenz der Business Services (aus Sicht der Kunden)
- End-to-end Sicht der Business Services und deren Abhängigkeiten sowie relevante Risiken
- Etablierung von Überbrückungslösungen zur Weiterführung der Business Services

- Ownership für Themen wie Access Management und Datenschutz
- Einbezug von Cyber-Spezialisten mit einem Sitz am Tisch einer Business-/Produkt-Idee von Tag 1 an
- Wiederverwendung von standardisierten Komponenten

# Konklusion

Cyber entwickelt sich weiterhin rasant und die Kundenerwartungen steigen. Es ist eine Herausforderung für alle, mit diesen Änderungen Schritt zu halten. Es bleibt deshalb wichtig, den Fokus auf die wesentlichen Aspekte nicht zu verlieren.

## Fokus-Themen einer zeitgemässen Cyber-Strategie


## Erfolgsfaktoren einer effektiven Umsetzung

- Risiken verstehen und bewusst eingehen
- Handeln, statt nur konzipieren
- Alle übernehmen Verantwortung
- Cyber wird zu messbaren persönlichen Zielen
- Investments in eigenes Cyber-Talent

# Kontakte


Reto Häni
rhaeni@deloitte.ch
Partner | Europäischer Leiter Cloud Security und Risk
Deloitte Schweiz



Florian Widmer
fwwidmer@deloitte.ch
Partner | Leiter Cyber Resilience
Deloitte Schweiz



Frank Walter
fwalter@deloitte.ch
Director | Cyber Resilience
Deloitte Schweiz

Deloitte.