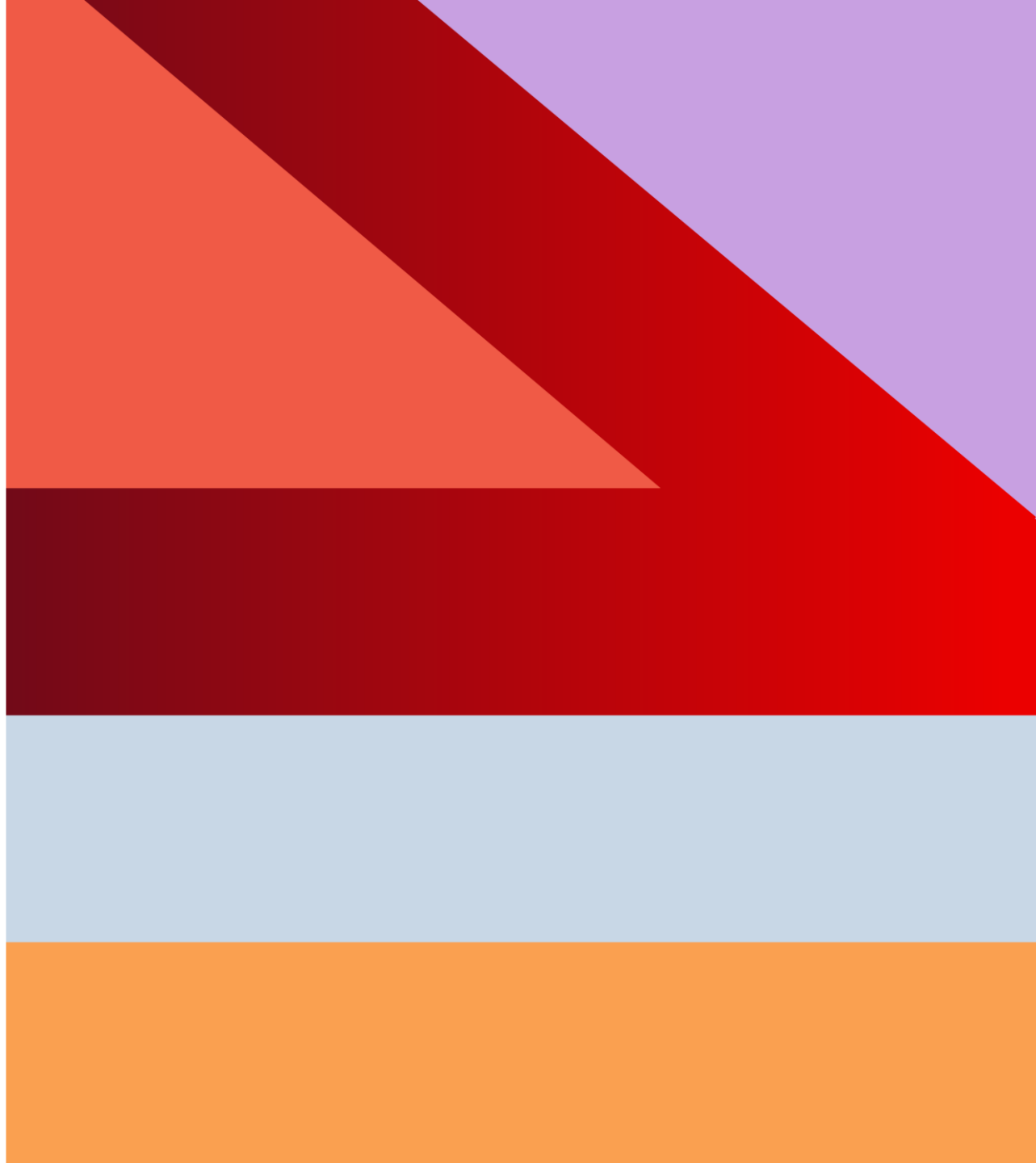
Cyberangriffe auf Spitäler – Best Practices

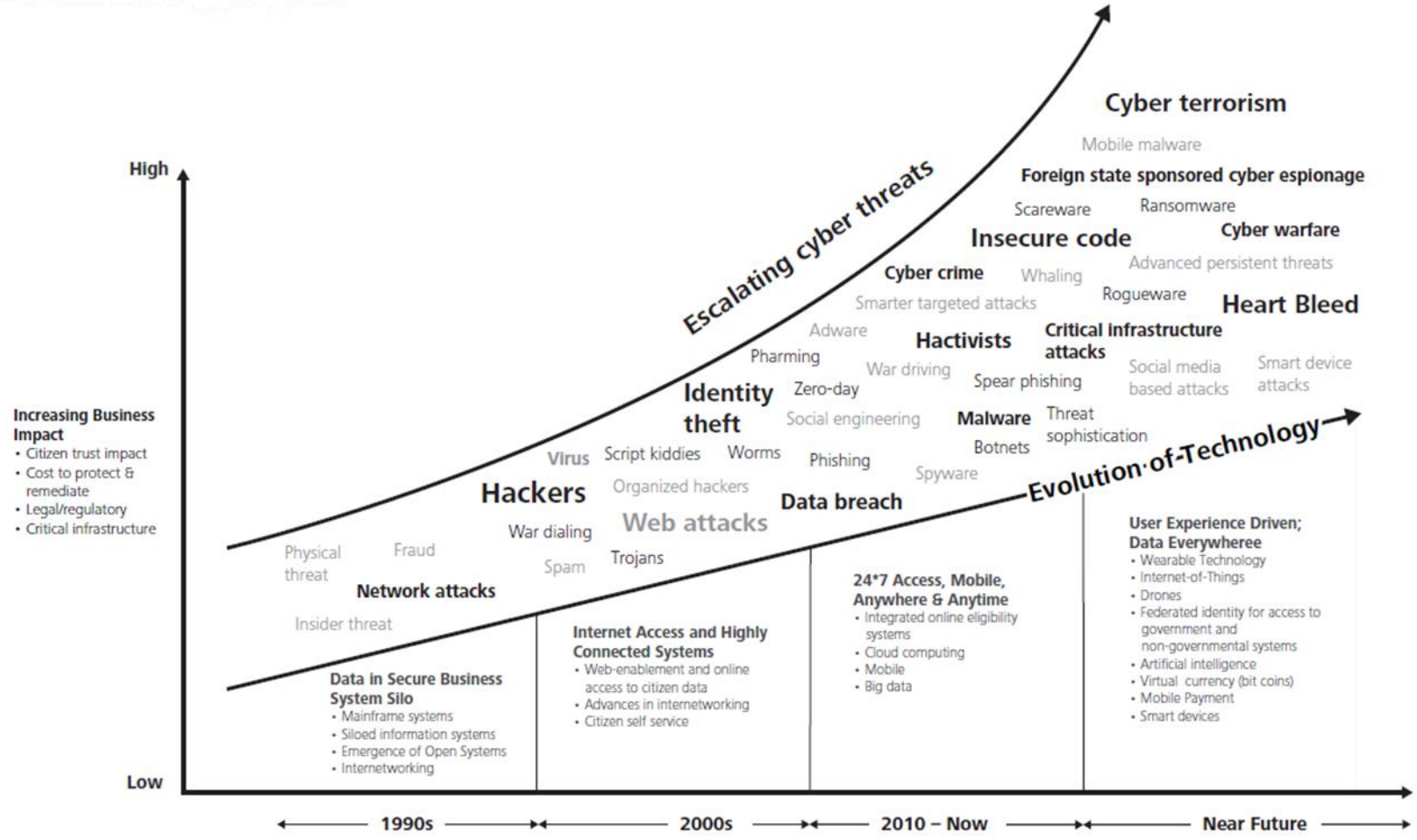
Lukas Bühlmann
15. April 2023

Agenda

1. Intro
2. Grösste Bedrohungen
3. Risikofaktor Mensch
4. Best Practice – IT Readiness
5. Best Practice – PR Readiness
6. Best Practice – Legal Readiness
7. Compliance Checkliste
8. FAQ



Changing Cyber Threats



Intro

- Spitäler sind Teil der kritischen Infrastruktur
- Hoch-sensitive Daten
- IT: Hohe Dependenz & dramatische Folgen bei Ausfall
- Hohes öffentliches Aufsehen bei Ausfall Spital
- Schutz & Awareness gegen Cyberattacken i.d.R. unzureichend

Attraktivität als Ziel enorm für Cyberkriminelle

Grösste Bedrohungen aktuell

- Ransomware
- Zero-Day-Exploits
- Sabotage
- Spionage

Cyberattacken auf Spitäler sind kein theoretisches Risiko….

Zum Beispiel:

2021: Cyberangriff Health Service Executive (HSE) in Irland

- Verantwortung für alle öffentlichen Gesundheitsdienstleistungen in Irland (an 4000 Orten, mit 54 Spitälern und mehr als 70 000 Geräten wie Laptops und PCs) und mit 130 000 Angestellten die grösste Arbeitgeberin des Landes.
- Um die Auswirkungen des Cyberangriffs einzudämmen und zu bewerten, hat die HSE im Rahmen ihres "Critical Incident Process" (Prozess für kritische Vorfälle) sofort all ihre IT-Systeme abgeschaltet und das nationale Gesundheitsnetz vom Internet getrennt.
- Folge, dass das Gesundheitspersonal keinen Zugang mehr zu den von der HSE bereitgestellten IT-Systemen hatte – einschliesslich Patienteninformationssysteme, klinische Versorgungssysteme, Laborsysteme und nicht-klinische Systeme wie Finanzen, Lohnabrechnung und Beschaffung.
- Dauer zur Wiederherstellung der Systeme einige Monate.

Risikofaktor Mensch

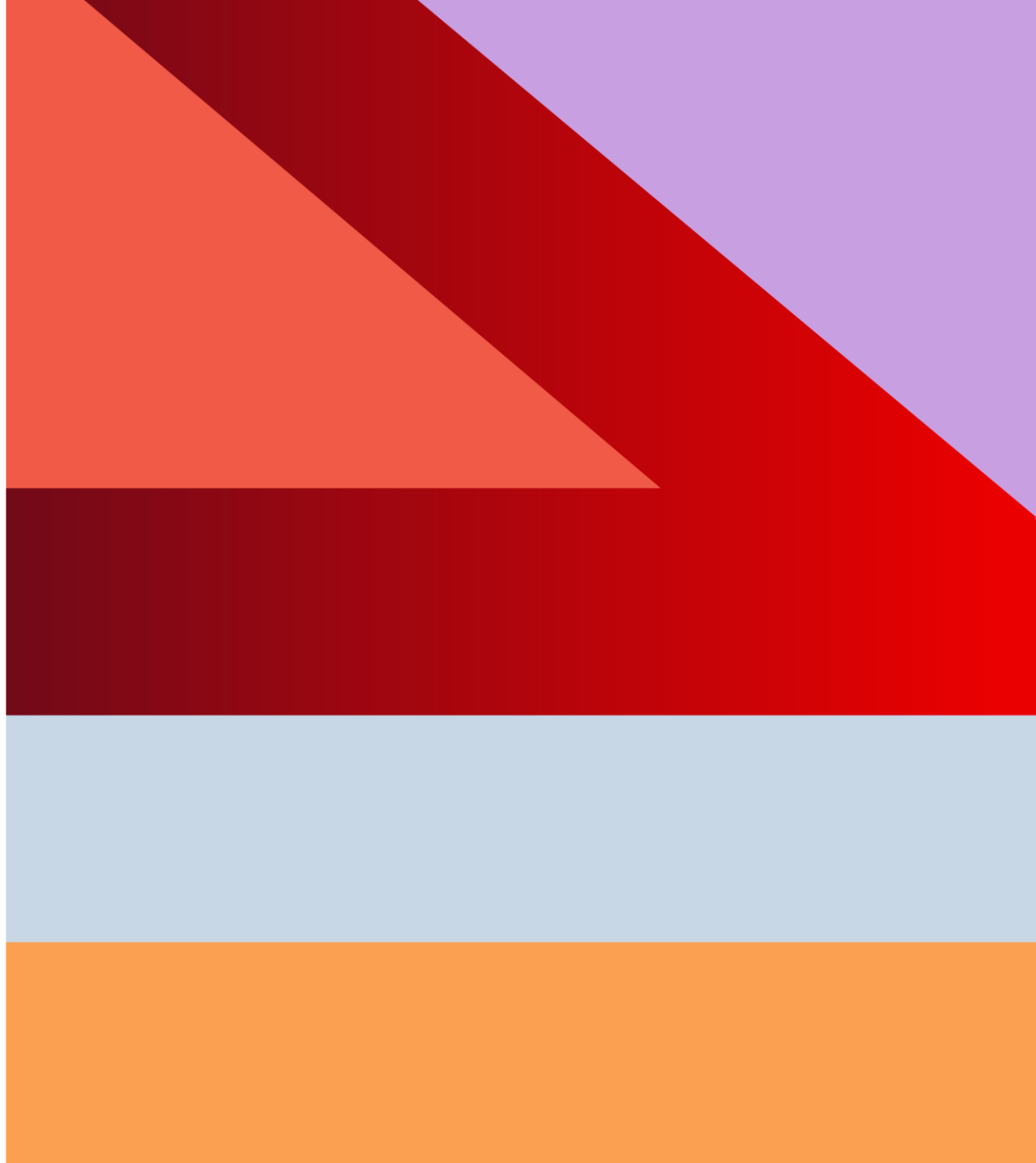
Grösste Risikofaktoren / Einfallstore:

- Social Media
- Phishing
- Passwörter
- Schatten-IT
- Fehlerkultur

Enorme Kostenfolgen

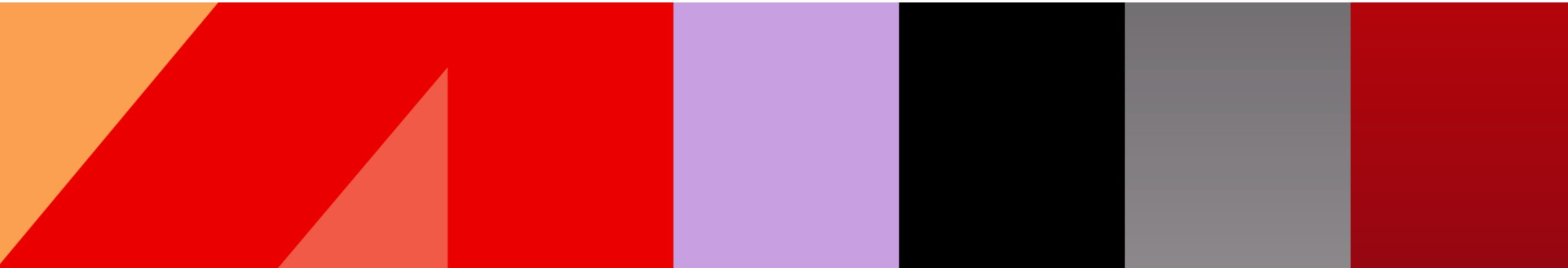
Die mit einer Cyber-Attacke direkt verbundenen Kosten belaufen sich auf:

- CHF 250K (KMU) bis CHF 7-8 Mio. (bei ca. 2’000 Mitarbeiter)
- Exkl. Reputationsschäden
- Exkl. Ransom-Zahlung



Was ist zu tun?

Best Practices



Best Practices – IT Incident Readiness

- Vorbereitung
  - Rechnen Sie damit, dass Sie ein interessantes Ziel sind
  - Inventur und Verständnis, was im Unternehmen «digital» passiert
  - Verantwortlichkeiten und Zuständigkeiten definieren inkl. Stellvertretung
  - Eskalationspfad definieren inkl. Entscheidungsträgern
  - Dokumentieren (physisch)
- Training
  - Kontinuierliches Training macht ein Unternehmen stärker
  - Das Team kennt die Tools
  - Das Team kennt die Abhängigkeiten und Funktionsweisen der Tools
  - Wissen, was man tut
  - «Was passiert wenn» Szenarien trainieren

Best Practices – IT Readiness

- Ernstfall planen
  - Erstellen eines Incident Response Planes
  - Soviel Informationen wie möglich sammeln
  - Entscheidungen basierend auf Fakten treffen
  - Entscheidungsträger involvieren
  - Konsequenzen von Entscheidungen evaluieren und in ein Verhältnis zum Risiko setzen
  - Incident Response Strategie mehrfach überprüfen und ggf. anpassen
  - Experten beiziehen

Best Practices – PR Incident Readiness

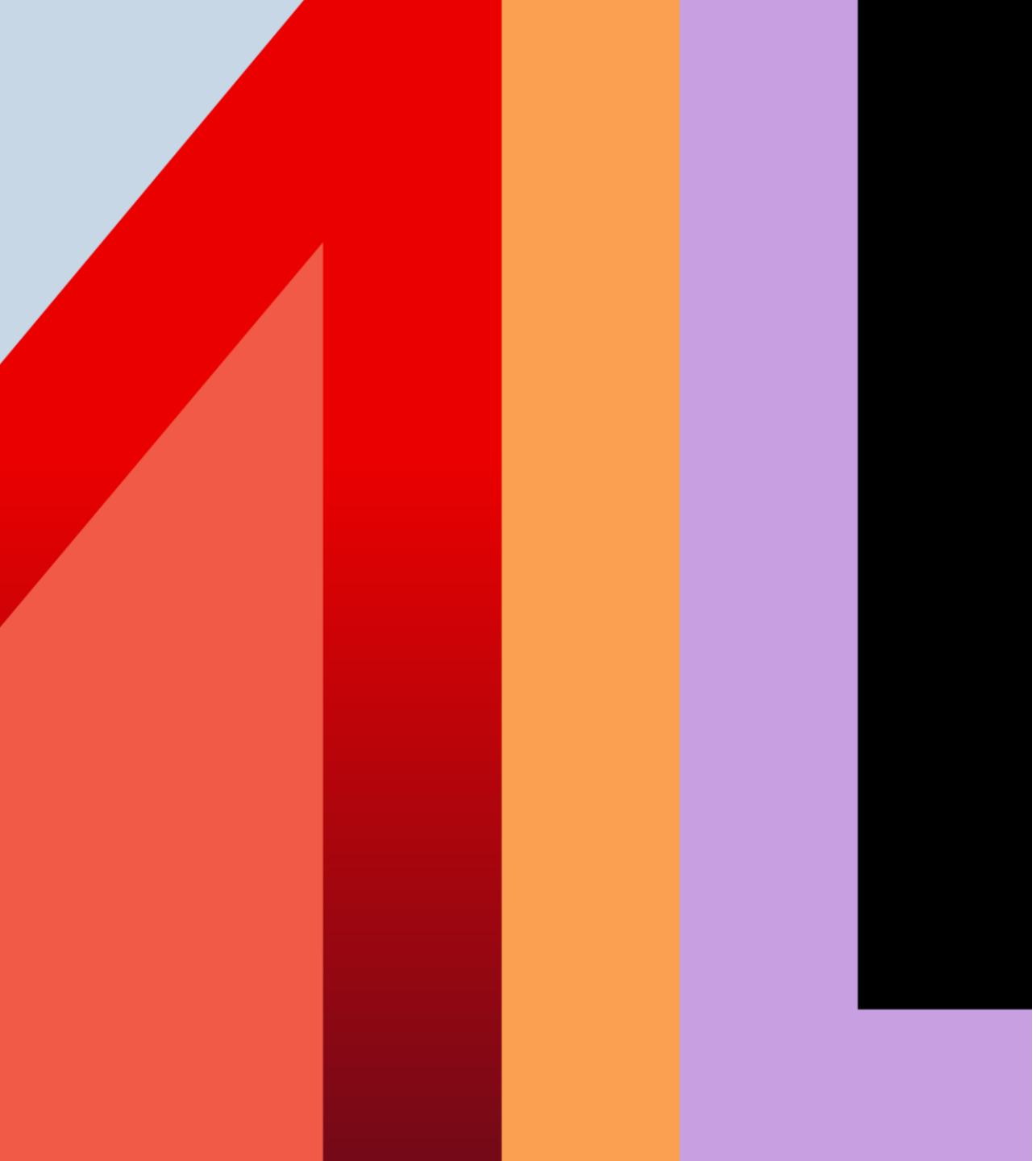
Was auf dem Spiel steht….

Best Practices – PR Incident Readiness

- Inhaltliche Vorbereitungen für die Krisenkommunikation
  - Kontaktdaten zu 24/7 Stand-by Service
  - Quick Reaction Team / Führungsstab
  - Liste von Sofortmassnahmen
  - Checklisten, Hilfsblätter & Formulare
  - Kontaktlisten diverse Stakeholder
  - Templates für Medienmitteilungen
  - Blueprints für Social Posts
  - Kommunikations-Richtlinien
  - Ereignis Journal für Events in On- und Offlinemedien
  - Notfall-Website
  - …

Best Practices – PR Incident Readiness

- Typische Stakeholder Krisenkommunikation
  - Medien
  - Eigner
  - Mitarbeiter
  - Patienten
  - Behörden
  - Bevölkerung
  - Geschäftspartner
  - NGOs
  - Opinion Leaders



Cybersecurity & Recht im Gesundheitssektor

Cybersecurity – Legal Readiness Topics

- State-of-the-Art Datensicherheit als Compliance Voraussetzung (aufgrund diverser Regulierungen)
- Meldepflichten
  - An Datenschutzbehörden
  - An Aufsichtsbehörden & Regulatoren
  - An Betroffene Personen
  - An Kreditkarten- und Finanzunternehmen
  - An Vertragspartner
  - An Versicherungen
- Ransom sums
- Haftung
- Versicherungsdeckung

Art. 8 revDSG:

Art. 8 Datensicherheit

[1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

[2] Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

[3] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Strafsanktionen - Art. 61 revDSG:

Art. 61 Verletzung von Sorgfaltspflichten

Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich:

a. unter Verstoss gegen Artikel 16 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 17 erfüllt sind, Personendaten ins Ausland bekanntgeben;

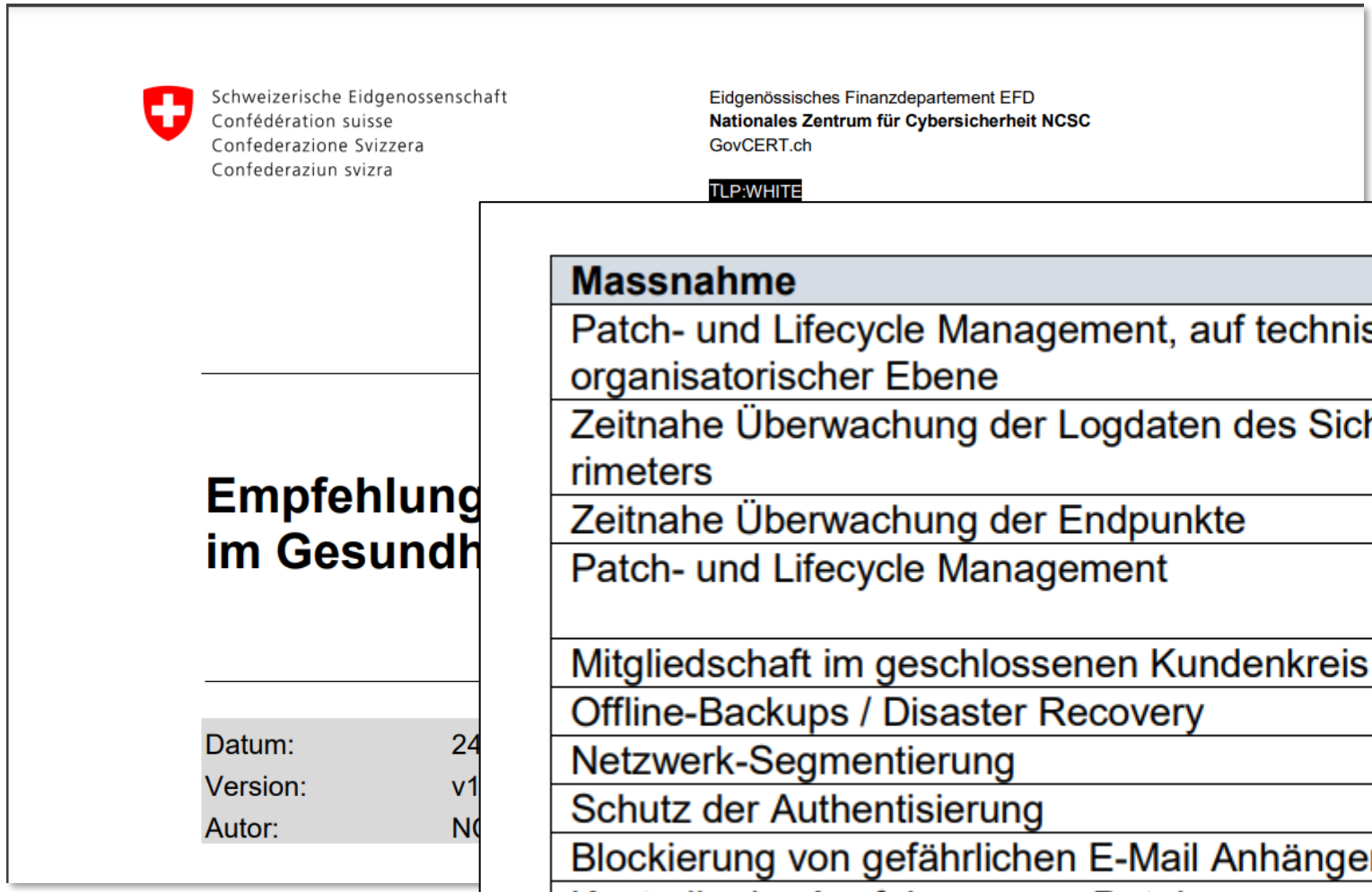
b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 9 Absätze 1 und 2 erfüllt sind;

c. die Mindestanforderungen an die Datensicherheit, die der Bundesrat nach Artikel 8 Absatz 3 erlassen hat, nicht einhalten.

“Angemessene Datensicherheit”

- Dynamischer Begriff, branchen- und unternehmensspezifiisch
- Mögliche Orientierungspunkte:
  - Swiss ICT Minimum Standards
  - Empfehlungen NCSC zur Cybersicherheit im Gesundheitssektor (Mai 2022)
- Sog. Technische und Organisatorische Massnahmen (TOM’s)
- Regelmässig zu überprüfen und anzupassen!

NCSC: TOM’s für den Gesundheitssektor


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
GovCERT.ch

TLP:WHITE

Empfehlung
im Gesundh

Datum: 24
Version: v1
Autor: NC

Massnahme	Umsetzung	Vorgabe
Patch- und Lifecycle Management, auf technischer und organisatorischer Ebene	Organisatorisch	Muss
Zeitnahe Überwachung der Logdaten des Sicherheitsperimeters	Organisatorisch und Technisch	Muss
Zeitnahe Überwachung der Endpunkte	Technisch	Kann
Patch- und Lifecycle Management	Organisatorisch und Technisch	Muss
Mitgliedschaft im geschlossenen Kundenkreis des NCSC	Organisatorisch	Kann
Offline-Backups / Disaster Recovery	Technisch	Muss
Netzwerk-Segmentierung	Technisch	Muss
Schutz der Authentisierung	Technisch	Muss
Blockierung von gefährlichen E-Mail Anhängen	Technisch	Kann
Kontrolle der Ausführung von Dateien	Technisch	Kann

Meldepflichten

Meldepflicht - Datenschutzgesetz

- Legaldefinition des Begriffs der Verletzung der Datensicherheit:
- *«(…) eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden»*
- Pflicht zur Meldung beim EDÖB, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt
- «so rasch als möglich»: Keine explizite Zeitangabe
  > Orientierung an DSGVO (72h) sinnvoll
- U.U. Meldung an betroffene Personen
- **Neu:** Pflicht zur Meldung von Verletzungen der Datensicherheit

Neue Meldepflicht - Informationssicherheitsgesetz

- Meldepflicht Cyberangriffe durch Betreiber kritischer Infrastrukturen an das Nationale Zentrum für Cybersicherheit (NCSC).
- Inkrafttreten 2023 parallel zum revDSG (1. September 2023)
- Gesundheitseinrichtungen auf der kantonalen Spitalliste (neben Spitälern auch Geburtshäuser und Pflegeheime) gelten gem. ISG als kritische Infrastrukturen
- Cyberangriffe sind zu melden, wenn:
  - Gefährdung der Funktionsfähigkeit der betroffenen kritischen Infrastruktur
  - Manipulation oder Abfluss von Informationen
  - Angriff unentdeckt über einen längeren Zeitraum, insb. wenn Anzeichen dafür bestehen, dass er zur Vorbereitung weiterer Cyberangriffe ausgeführt wurde; oder
  - mit Erpressung, Drohung oder Nötigung verbunden ist und diese einen Bezug zum meldepflichtigen Unternehmen hat und sich auf dessen Geschäftstätigkeit negative auswirken kann.

Neue Meldepflicht - Informationssicherheitsgesetz

Inhalt der Meldung

- Informationen zur meldepflichtigen Behörde oder Organisation,
- zur Art und Ausführung des Cyberangriffs (z.B. IP-Adressen oder DNS-Records von bekannten Angriffsinfrastrukturen wie etwa Botnetze oder von Command and Control-Servern, URL zu verdächtigen Seiten, hash-Werte von Malware, Virensignaturen, Anomalien im Netzwerkverkehr oder verdächtiges Verhalten von Software),
- zu den Auswirkungen,
- zu ergriffenen Massnahmen, und
- soweit bekannt, zum geplanten weiteren Vorgehen.
- Ausgeschlossen: keine Angaben, die zu einer strafrechtlichen Belastung des Meldenden führen könnte.

Neue Meldepflicht - Informationssicherheitsgesetz

Meldefrist:

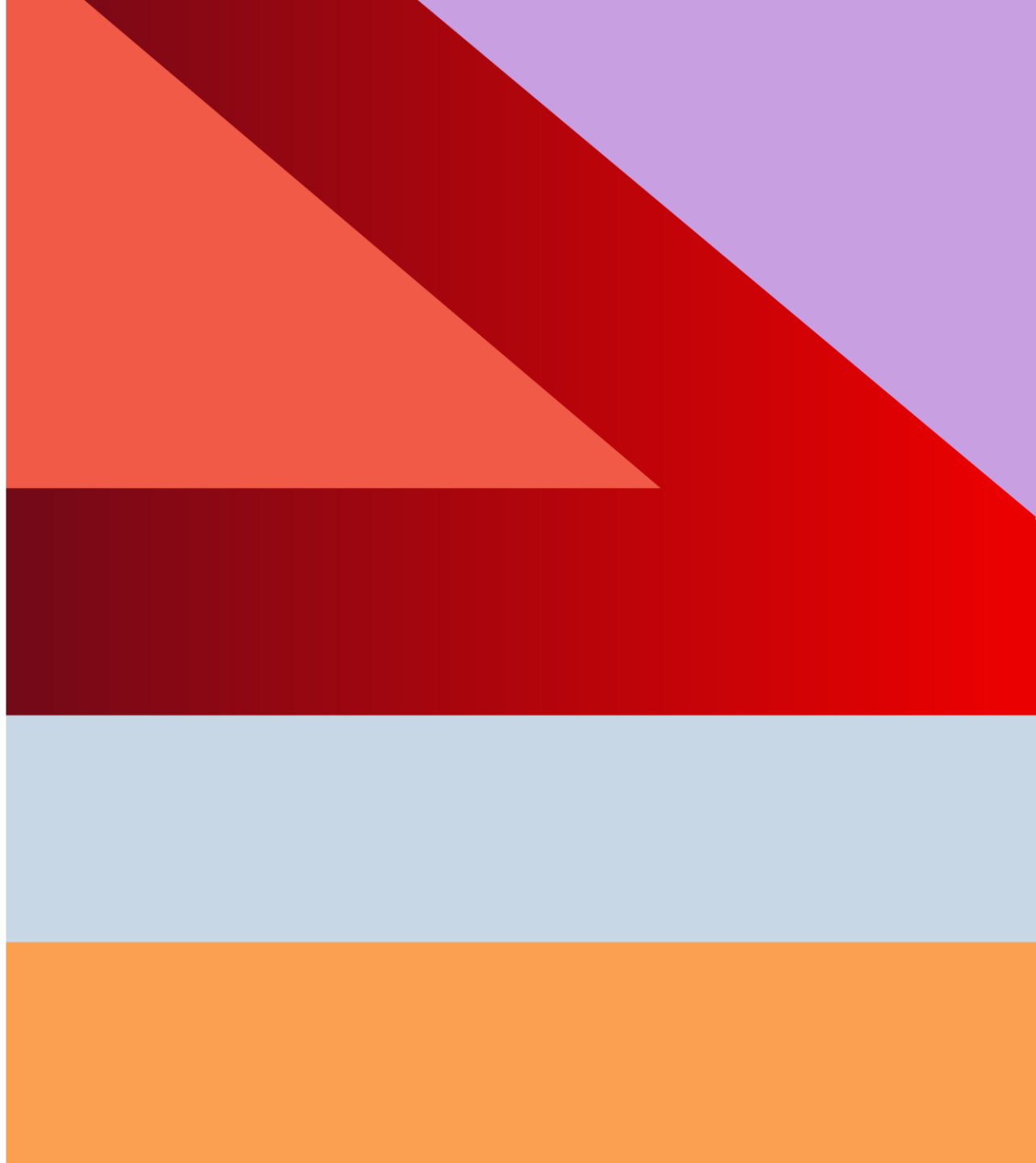
- Innerhalb 24 Stunden nach Entdeckung Cyberangriff
- Alle Informationen, die bis dahin bekannt sind
- Nachmeldung, sofern notwendig

Strafbestimmungen:

- Unterlassung der Meldung nicht strafbar
- Widerhandlung gegen Verfügung NCSC strafbar, Busse bis CHF 100’000
- Person «die innerhalb der kritischen Infrastruktur hätte dafür sorgen müssen, dass der Verfügung des NCSC Folge geleistet wird»

Ransomware

- Darf man überhaupt ein Ransom zahlen?
- Aufpassen – die Zahl der «Double-dipping» Attacken nimmt zu
  - Eine Zahlung um verschlüsselten Daten frei zu bekommen
  - Eine Zahlung um eine Veröffentlichung von Daten zu verhindern

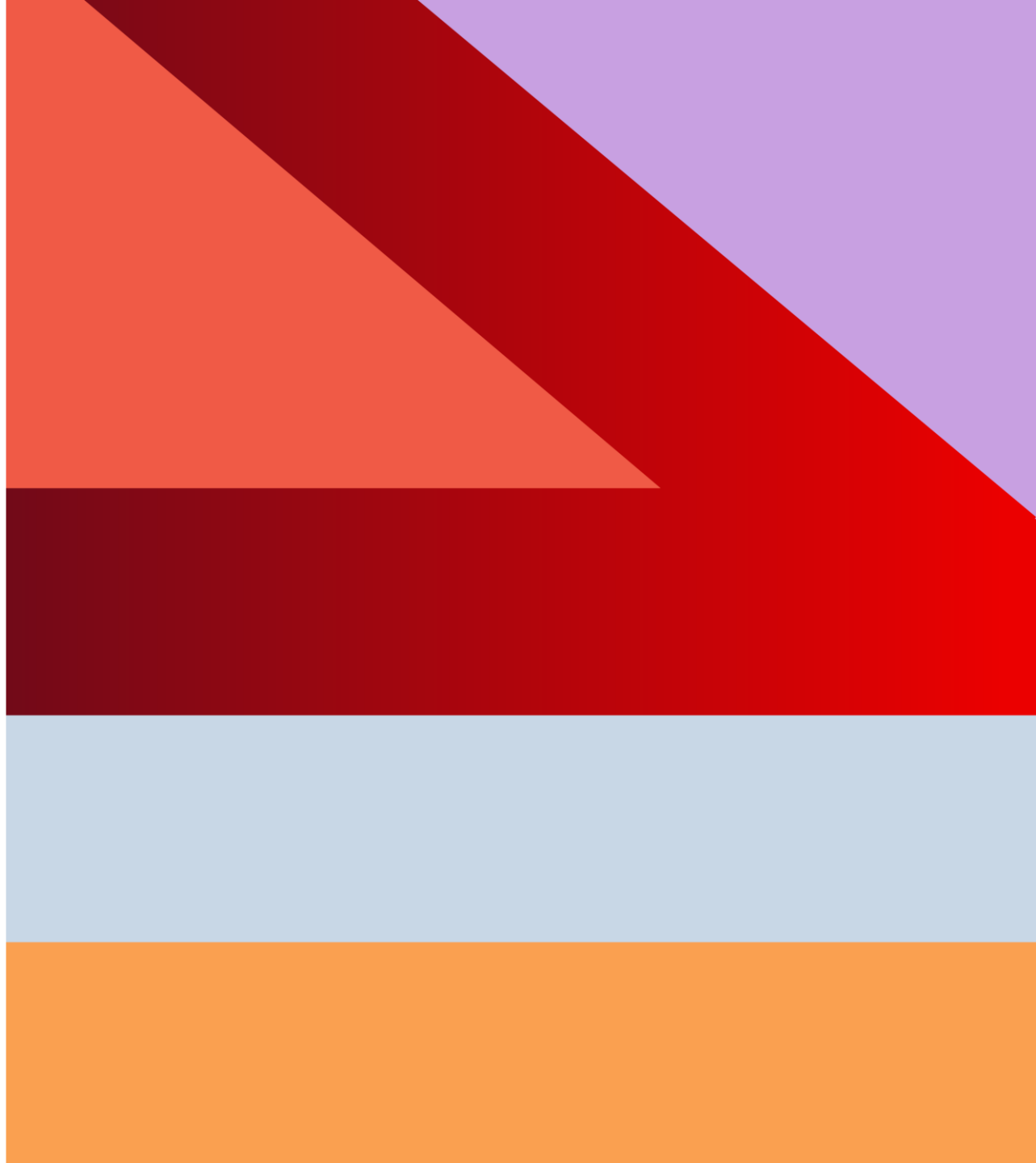


Wer kann haftbar gemacht werden?

- **Der Datenverantwortliche**
- Verletzung der Pflicht, Datensicherheit zu gewährleisten oder zu vergewissern, dass die Datensicherheit beim Auftragsbearbeiter gewährleistet ist.
- Vertragsrechtliche Pflichten gegenüber Kunden oder anderen.
- **Der Auftragsbearbeiter**
- Verletzung der Pflicht, Datensicherheit zu gewährleisten.
- **Die Bank**
- Sorgfaltspflicht bei der Ausführung von Instruktionen.
- **Der Verletzer**

Compliance Checkliste

- ✓ Policy für Datenschutzverletzungsfälle
- ✓ Interne Verantwortlichkeiten und Meldestellen definieren
- ✓ IT-Sicherheitsaudits und Response-Übungen durchführen
- ✓ Datenschutz-Compliance
- ✓ Mitarbeiterschulungen
- ✓ Versicherungsschutz
- ✓ Kommunikationsmassnahmen vorbereiten



Lukas Bühlmann, LL.M.
Partner, Co-Head ICT & Digital, Zürich
lukas.buehlmann@mll-legal.com
www.mll-legal.com

Vielen Dank für Ihre Aufmerksamkeit!

Über MLL Legal

MLL Legal ist eine der führenden Anwaltskanzleien in der Schweiz mit Büros in Zürich, Genf, Zug, Lausanne, London und Madrid. Wir beraten unser Klientel in allen Bereichen des Wirtschaftsrechts und zeichnen uns insbesondere durch unsere erstklassige Branchenexpertise in technisch-innovativen Spezialgebieten, aber auch in regulierten Branchen aus.

Internationale Ausrichtung

Wir denken kosmopolitisch und bieten massgeschneiderte, grenzüberschreitende Lösungen für unsere Schweizer und internationalen Mandanten.

Juristische Exellenz

Unsere Expertinnen und Experten finden sich in den bedeutenden internationalen Anwaltsrankings stets an vorderster Stelle.

Flexible Teams

Wir sind eine voll integrierte Kanzlei mit einer interdisziplinären Denkweise und einem starken Teamgeist.

Vielfalt und Nachhaltigkeit

Vielfalt und Toleranz sind fest in unserer Firmenkultur verankert und schaffen die geistige Unabhängigkeit, die unsere Klientinnen und Klienten von ihren Anwältinnen und Anwälte erwarten dürfen

Unsere strategischen Positionierungen und Stärken: Schnittpunkt von High-Tech, IP-reichen und regulierten Branchen