Digitale Resilienz

Ransomware und DORA

Andreas Rostin

Roman Regenbogen

Zürich, 8. Mai 2024

Die Evolution von Ransomware

Von Ransomware zu Double Extortion Ransomware

Ransomware

- Malware, mit der Daten auf Computern oder Netzwerken von Kriminellen verschlüsselt werden
- Forderung von Lösegeld, um den Zugriff wiederherzustellen

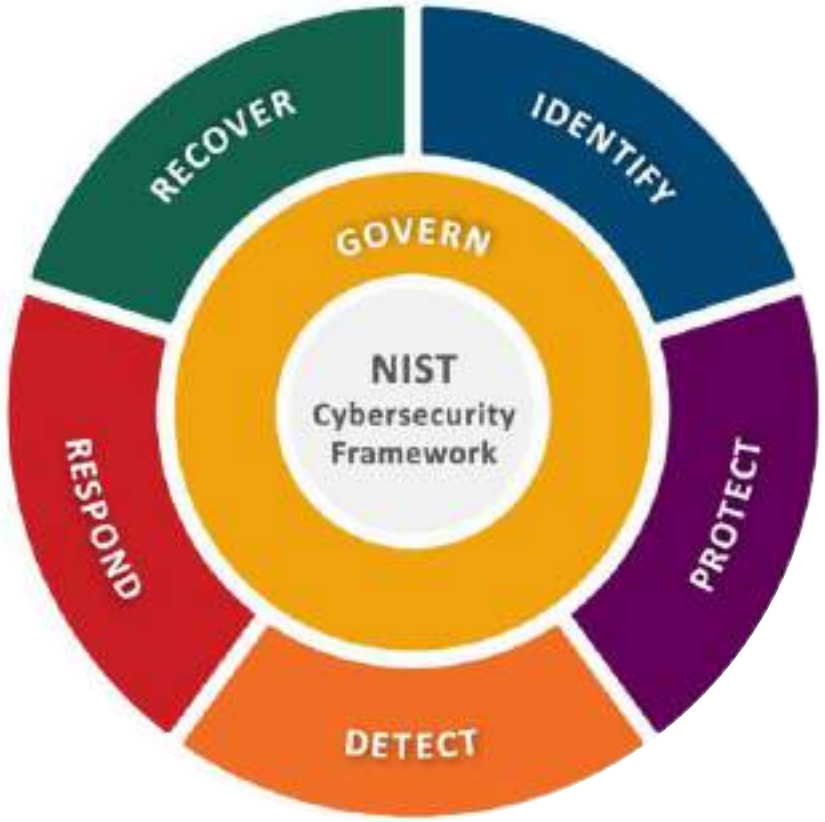
Extortionware

- Malware, mit der vertrauliche Daten gestohlen werden
- Drohung, diese Daten zu veröffentlichen oder anderweitig zu nutzen, sofern keine Zahlung geleistet wird

Double Extortion Ransomware

- Kombination aus beiden Angriffstypen
- Angreifer verschlüsseln Daten und stehlen gleichzeitig eine Kopie
- Angreifer fordern Lösegeld und drohen, die Daten zu veröffentlichen

Was kann ich als Unternehmen tun, um mich zu schützen?



GOVERN: Third-Party Cyber Risk Management

IDENTIFY: Vulnerability and Patch Management

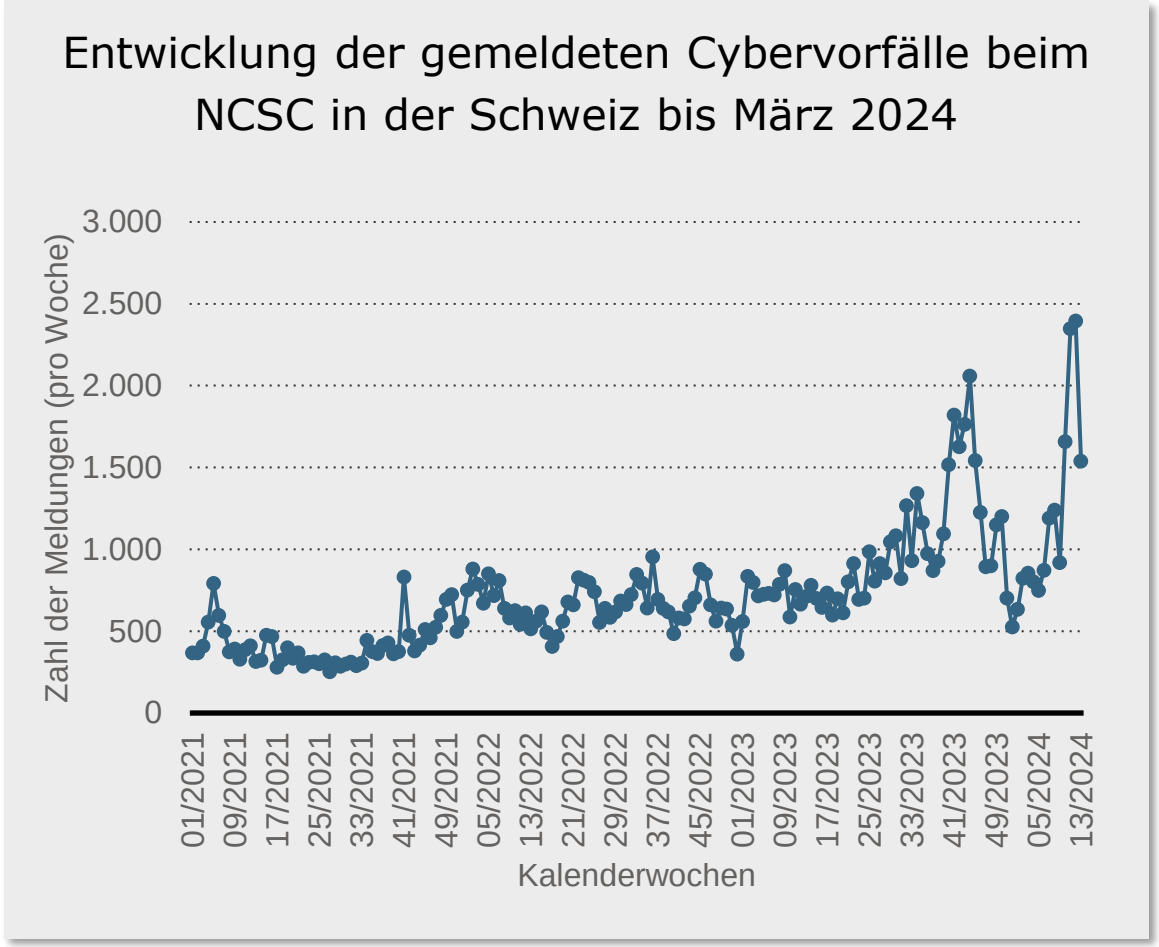
PROTECT: Multi-Factor Authentication & Employee Awareness

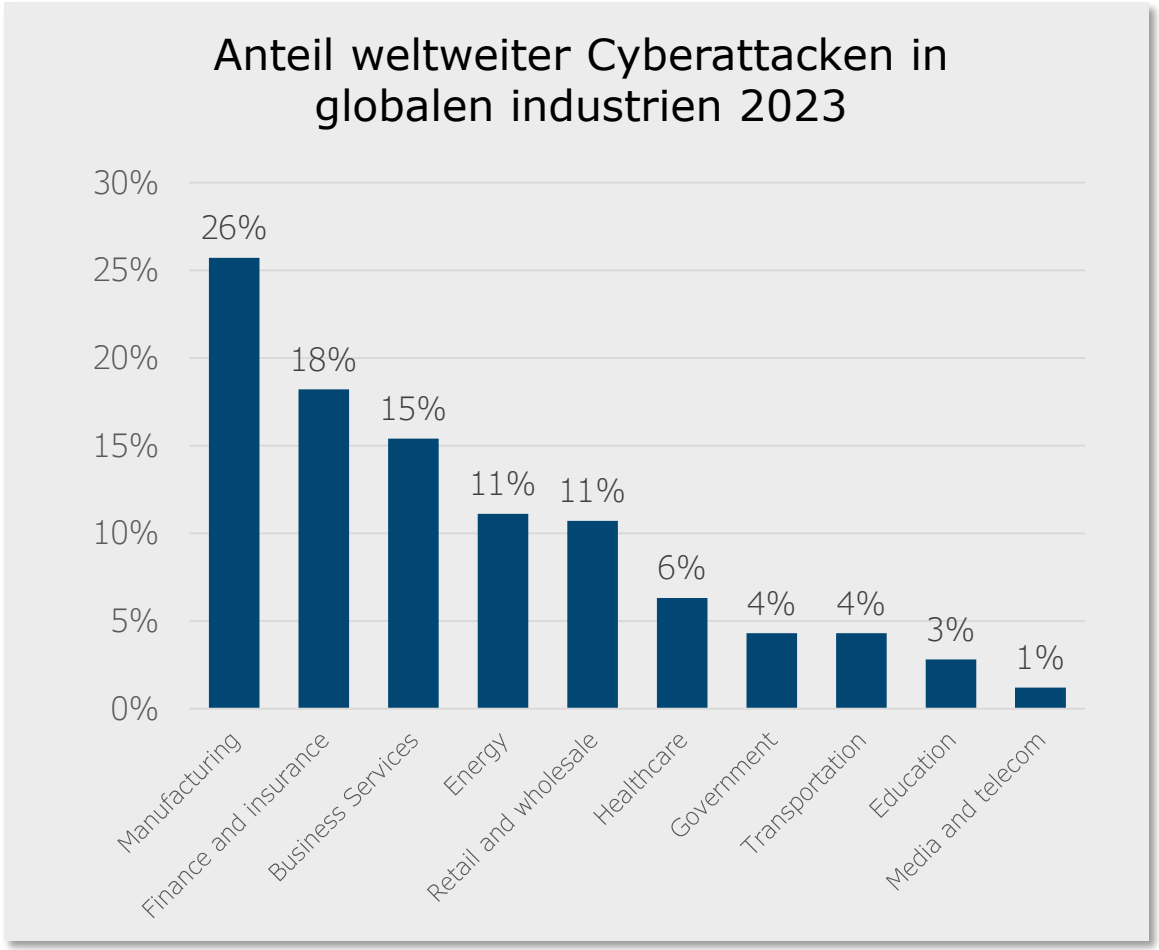
DETECT: Continuous Monitoring & Event Analysis

RESPOND: Incident Response Plan

RECOVER: Backup and Recovery Strategy

Ransomware betrifft alle Industrien, jedoch mit unterschiedlicher Ausprägung





Quelle: Statista.com

Was ist der Digital Operational Resilience Act (DORA)?

eraneos

Ziel der DORA ist die Förderung innovativer Technologien bei zeitgleicher Sicherstellung der digitalen Betriebsstabilität

D — **Digital**
Technologie und Daten sind essentielle Veränderungstreiber im Finanzsektor und bieten sowohl Chancen als auch Risiken.

O — **Operational**
Die Betriebsstabilität digitaler Systeme soll durch standardisierte Sicherheitsanforderungen gewährleistet werden.

R — **Resilience**
Eine konsequente Bewertung und proaktive Bewältigung von Risiken begrenzt potenziell katastrophale Folgen eines Incidents.

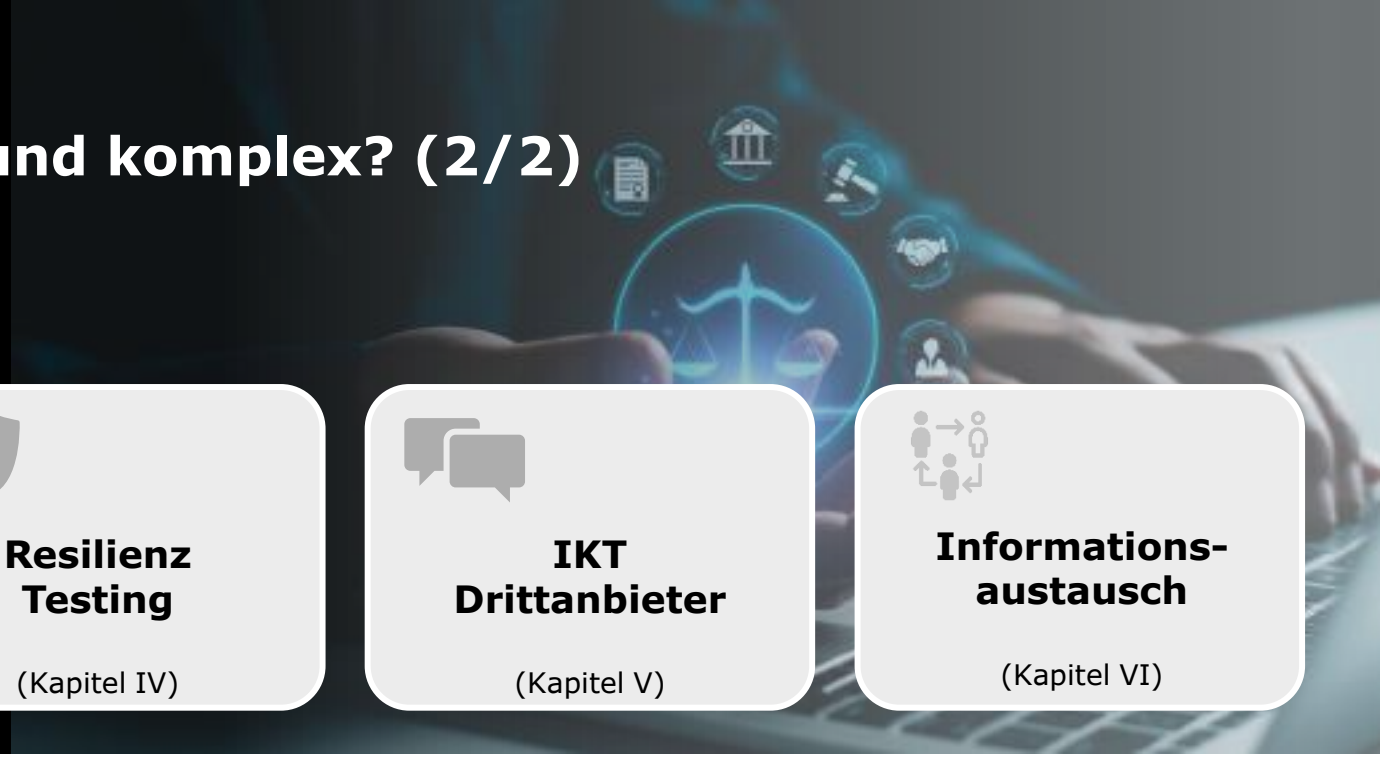
A — **Act**
Zum kontinuierlichen Schutz der Verbraucher und Finanzinstitute rückt die digitale Betriebsstabilität im Finanzsektor in den Fokus der Bankenaufsicht.

Was macht die DORA so einzigartig und komplex? (1/2)

Geltungsbereich der DORA

- **Unternehmen der Finanzbranche**
  - Kreditinstitute
  - Versicherungen
  - Krypto-Dienstleister
  - Schwarmfinanzdienstleister
  - …
- **IKT-Drittdienstleister**
  - SW-/HW-Anbieter
  - Anbieter von Telekommunikation
  - Anbieter von Cloud-Diensten
  - Rechenzentren
  - …
- In der **EU-tätige Unternehmen**, auch wenn diese ihren Hauptsitz z.B. in der Schweiz oder Grossbritannien haben
- **Proportionalitätsprinzip** findet Anwendung

Was macht die DORA so einzigartig und komplex? (2/2)



Wesentliche Anforderungen der DORA

IKT Risikomanagement

(Kapitel II)

- Einbindung und Schulung der Führungspersonen
- Erprobung von BCM Plänen (Notfallpläne)

IKT Vorfälle

(Kapitel III)

- Erkennung und Klassifizierung von Vorfällen
- Berichterstattung von IKT bezogenen Vorfällen an Behörden

Resilienz Testing

(Kapitel IV)

- Vorgaben für das operative Testing von IKT-Tools und Systemen
- Unabhängiges Threat-Led Penetration Testing (TLPL)

IKT Drittanbieter

(Kapitel V)

- Erweitertes Informationsregister für Drittparteien
- Exit- und Terminierungspläne vertraglich festlegen
- Schulung von Drittparteien

Informations-austausch

(Kapitel VI)

- Erkenntnisse über Cyberbedrohung
- Sammlung und Aufbereitung relevanter Daten aus diversen Bereichen

- Bei der Umsetzung konkreter Anforderungen können Frameworks wie NIST oder Standards wie ISO 27001 angewendet werden.

Welche Empfehlungen und „good practices“ gibt es für die DORA Umsetzung?

Start

Anwendbarkeits-analyse

Initiieren Sie ein Projekt, mobilisieren Sie inter-disziplinäre Experten

Defizit Analyse

Dokumentieren Sie ihre Analyse zur Anwendbarkeit sowie deren Auswirkungen auf z.B. Geschäfts-aktivitäten und Standorte

Planung der Implementierung

Klären Sie die Abgrenzung von kritischen und wichtigen Funktionen frühzeitig

Implementierungs-phase

Berücksichtigen Sie laufende Initiativen und andere Regulierungen bei der Planung von Massnahmen und der Priorisierung eines Fahrplans

Ende

Fördern Sie durch die Umsetzungs-massnahmen eine Kultur für operationelle Resilienz

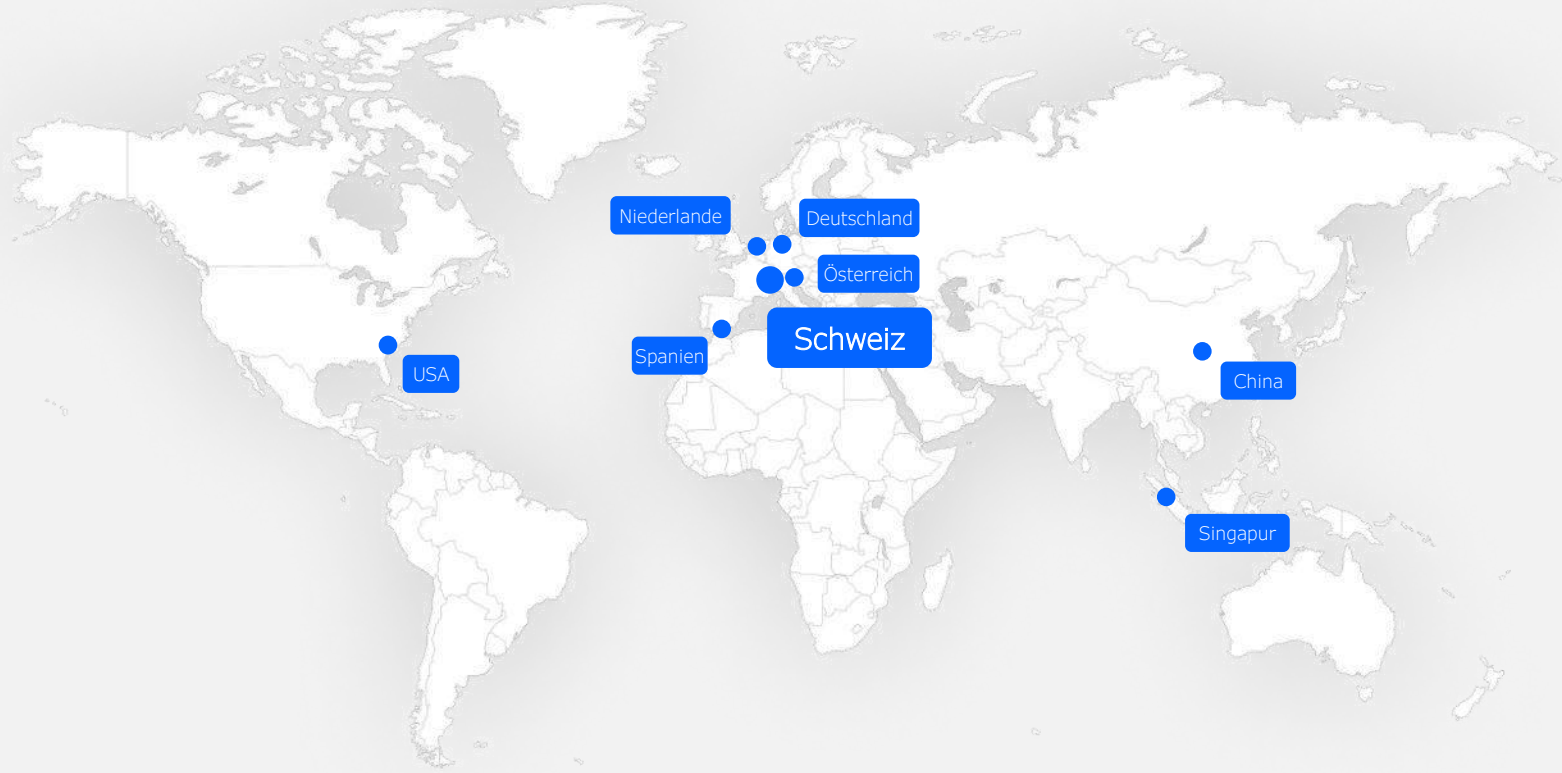
Überprüfung der Audit-Bereitschaft und regelmässige Resilienz Tests

Eraneos als Schweizer Management- und IT-Beratung hilft Kundinnen und Kunden, das volle Potenzial des digitalen Zeitalters zu nutzen.

13 Büros in acht Ländern

1100+ Engagierte Fachexperten

16 Industrien/ Branchen



Vertrauenswürdig

Uns vertrauen Fortune-500-Unternehmen, Regierungsorganisationen und Hidden Champions

Erfahren

Unsere Experten haben typischerweise mindestens 5 Jahre mehr Erfahrung pro Stufe

Kompetent

Wir stehen für erstklassige Beratung mit profundem Industriewissen und tiefer Technologie-Expertise

Ausgezeichnet

Wir sind ein führendes Beratungsunternehmen: 8x in Folge "Best Consultancy" Auszeichnung seit 2016

Lassen Sie uns sprechen

Gern stehen wir für Ihre Fragen zur Verfügung

Andreas Rostin
Cyber Security

andreas.rostin@eraneos.com
+41 76 283 8110

Roman Regenbogen
Regulatory & Compliance

roman.regenbogen@eraneos.com
+41 79 828 33 83