WEBINAR „INFORMATIONSSICHERHEITSGESETZ ISG“
SIND SIE BEREIT FÜR DAS NEUE ISG?

Reto Zbinden, CEO, Rechtsanwalt
Swiss Infosec AG | 5. Dezember 2023

INTEGRALE SICHERHEIT

RISIKOMANAGEMENT

INFORMATIONSSICHERHEIT

ISO 27001, ISMS, Informationsschutz, Archivierung

DATENSCHUTZ & IT-RECHT

Konformität nach DSG/DSGVO, Datenschutz-Folgenabschätzung, Personaldatenschutz, IT-Rechtsberatung, Data Breach

PERSONEN- UND PHYSISCHE SICHERHEIT

Arbeitssicherheit & Gesundheitsschutz, Facility Security, Evakuation, Brandschutz, Sensibilisierung, Ausbildung

IT-SICHERHEIT

Penetration Tests, Social Engineering, IT Security Reviews, DevSecOps, Cloud Security, IT-Sicherheitsprozesse und -architekturen

BUSINESS CONTINUITY MANAGEMENT

Notfall- und Krisenmanagement, ISO 22301, IT Service Continuity Management, Crisis Executive Assistance

ZIELE DES NEUEN INFORMATIONSSICHERHEITSGESETZES

- Umfassende, die **organisatorische und technische Seite** berücksichtigende Informationssicherheit zwecks **Stärkung der digitalen Resilienz**
- Festlegung **minimaler Sicherheitsanforderungen**
- **Zusammenfassung** der wichtigsten Massnahmen der Informations- und IT-Sicherheit in einer einzigen Regelung
- Umsetzung und Überprüfung integraler Informationssicherheit nach international anerkannten Standards (insbes. **ISO/IEC 27001** sowie **Standard des BSI**)
- Schaffung eines **formell-gesetzlichen Rahmens**, auf dessen Grundlage Bundesbehörden auf Verordnungs- und Weisungsebene Informationssicherheit einheitlich konkretisieren können
- Schliessung von **Lücken und Schwachstellen** des geltenden Rechts und dessen **Konsolidierung** (insbes. Informationsschutzverordnung, ISchV und Cyberrisikenverordnung, CyRV)
- Modernisierung der **Fachorganisation** der Informationssicherheit bei den Bundesbehörden
- Einführung einer **Meldepflicht** für Cyberangriffe auf kritische Infrastrukturen
- **Inkrafttreten** des ISG und der Ausführungsbestimmungen voraussichtlich **per 01.01.2024**

Das Informationssicherheitsgesetz ISG

schützt

- Informationen, für die Bund zuständig ist
- Informatikmittel des Bundes

verpflichtet

- Behörden und Organisationen des Bundes
- Organisationen, die Bundes-aufgaben wahrnehmen
- Betreiber kritischer Infrastrukturen *
- Kantone

verlangt

- Informations-sicherheit
- Risiko-management
- Zusammenarbeit mit Dritten
- Vorfall-management
- Klassifizierung
- IT-Sicherheit
- Personelle Massnahmen
- Physischer Schutz
- Identitätsverwal-tungssysteme
- Personensicher-heitsprüfung
- Betriebssicher-heitsverfahren
- Betrieb kritischer Infrastrukturen

* kritische Infrastrukturen sind:

- Behörden
- Energie
- Entsorgung
- Finanzen
- Gesundheit
- Information/Kommunikation
- Nahrung
- Öffentliche Sicherheit
- Verkehr

05.12.2023

SWISS INFOSEC

INFORMATIONSSICHERHEITSGESETZ
ISG-HAUS, UMSETZUNGSEMPFEHLUNGEN

Vorgaben → **Prozesse** → **Nachweise**

Informationssicherheit / Datenschutz / IT Sicherheit

Integrale Sicherheitspolitik
U.a. Informationssicherheit, Physische Sicherheit, Personelle Sicherheit, BCM

Weisung ISMS
Zielgruppe: GL, SiOrg, Informatik

Benutzerweisung
Zielgruppe: Alle MA

Merkblatt
Umgang mit klassifizierten Informationen

Sicherheitsregelwerk
IT-/OT-Sicherheit, IAM, personelle Massnahmen, physischer Schutz

IKT-Grundschutz

IT-Betriebsweisung
Strategie, Organisation, Prozesse

Templates
bspw. Sicherheitsverfahren, Data Breach

Umsetzung

Sicherheitsorganisation (u.a. ISV, ISB, DSB, Eigner)

Risiko Management

Sicherheitsverfahren/-prozesse
Klassifizierung, Schuban / ISDS-Konzept, (erw.) IKT-Grundschutz, Vorfallmanagement, Bearbeitungsreglement, Sicherheit in Projekten, Ausnahmen, Kontrollen, Audits, Berichterstattung

Zusammenarbeit mit Dritten
(Lieferantenmanagement)

Schulung / Sensibilisierung

Richtet sich an alle Mitarbeitende

Starker Bezug zu Datenschutz

Inventar der Schutzobjekte

Risikobehandlungsplan

Resultate/Dokumentation Sicherheitsverfahren/-prozesse

Audit-Berichte
IT/OT, ISMS, Lieferanten

Berichterstattung
(Management Reviews)

Betriebssicherheitsverfahren

Personensicherheitserklärung

IHRE PROBLEMLÖSUNG

beginnt mit einem Kontakt bei uns:

+41 41 984 12 12

infosec@infosec.ch

www.infosec.ch

Reto Zbinden
reto.zbinden@infosec.ch
+41 79 446 83 00

SWISS INFOSEC

VIELEN
DANK

MELDEN SIE SICH JETZT AN FÜR DIE KOSTENLOSE FACHVERANSTALTUNG

MEET SWISS INFOSEC!
Sicherheit im Fokus

Zürich Flughafen
13 bis 17 Uhr, anschliessend Apéro
www.infosec.ch/msi

Haben Sie schon den kostenlosen Newsletter abonniert?
www.infosec.ch/news

INFORMATIONSSICHERHEITSGESETZ QUELLEN – FEBRUAR 2023

- Botschaft BR vom Feb. 2017: https://www.admin.ch/opc/de/federal-gazette/2017/2953.pdf
- Erläuternder Bericht zum Ausführungsrecht vom 24. August 2022: https://www.newsd.admin.ch/newsd/message/attachments/72750.pdf
- Änderung des Bundesgesetz über die Informationssicherheit vom 2. Dezember 2022: https://www.fedlex.admin.ch/eli/fga/2023/85/de
- Botschaft zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen): https://www.fedlex.admin.ch/eli/fga/2023/84/de
- Regierungs- und Verwaltungsorganisationsgesetz (RVOG) betr. Geltungsbereich ISG: https://www.admin.ch/opc/de/classified-compilation/19970118/index.html
- Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022 (SKI): https://www.babs.admin.ch/de/aufgabenbabs/ski/nationalestrategie.html
- Kritische Infrastrukturen: https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html
- Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022: https://www.newsd.admin.ch/newsd/message/attachments/52071.pdf
- Nationale Cyberstrategie (NCS) 2023: https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/cyberstrategie-ncs/Nationale-Cyberstrategie-NCS-2023-04-13-DE.pdf.download.pdf/Nationale-Cyberstrategie-NCS-2023-04-13-DE.pdf