Cybersicherheit: Das neue Netz-und Informationssystemsicherheitsgesetz

Webinar 28. Februar 2019

Verena Becker

UBIT NIMMT WISSEN IN BETRIEB.

WKO WIRTSCHAFTSKAMMER NIEDERÖSTERREICH
Unternehmensberatung · Buchhaltung · IT

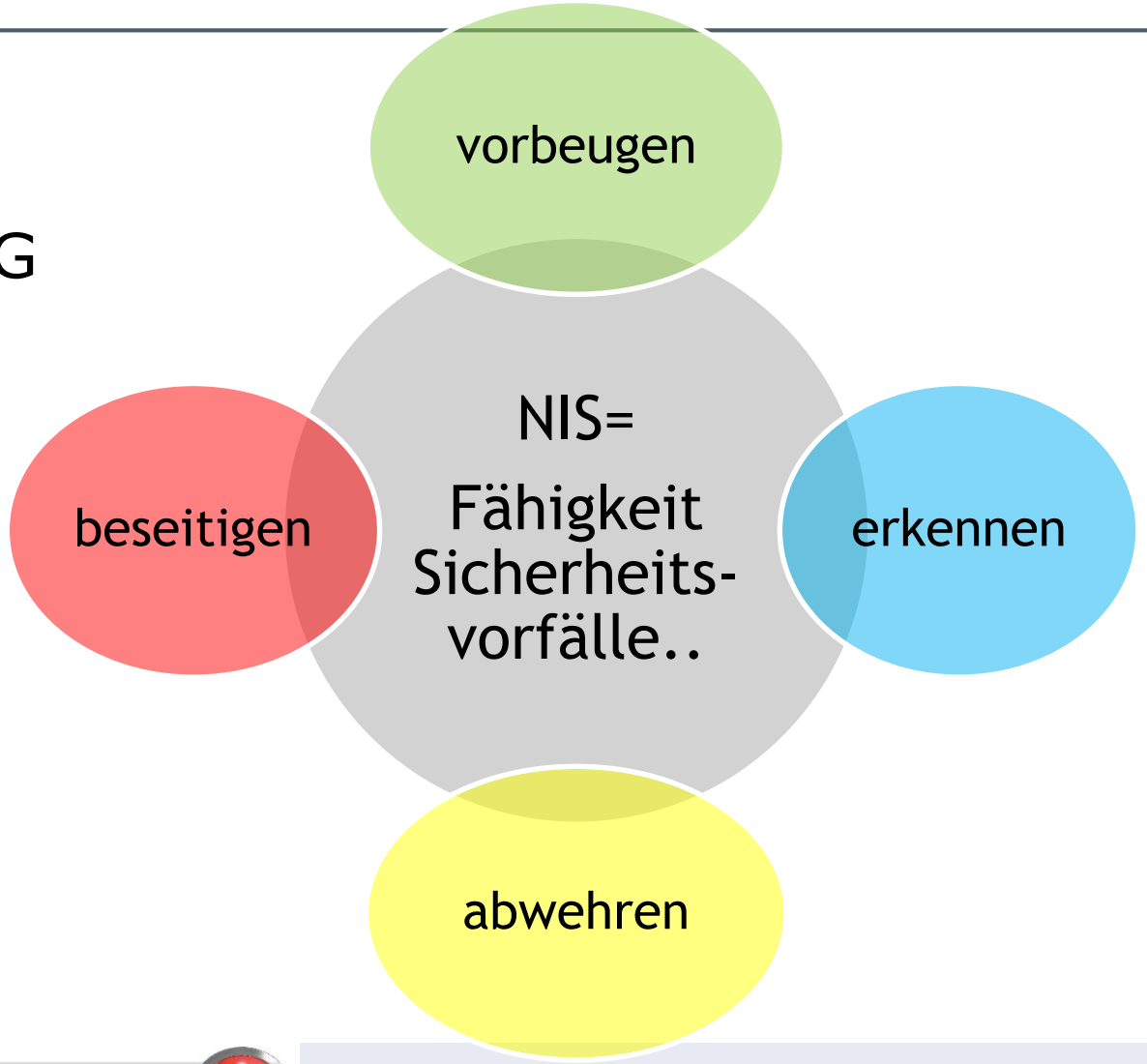
Inhalt

- Netz- und Informationssicherheit (NIS)
- Rechtsrahmen
- NIS-Richtlinie
- NISG

Vergleich DSGVO

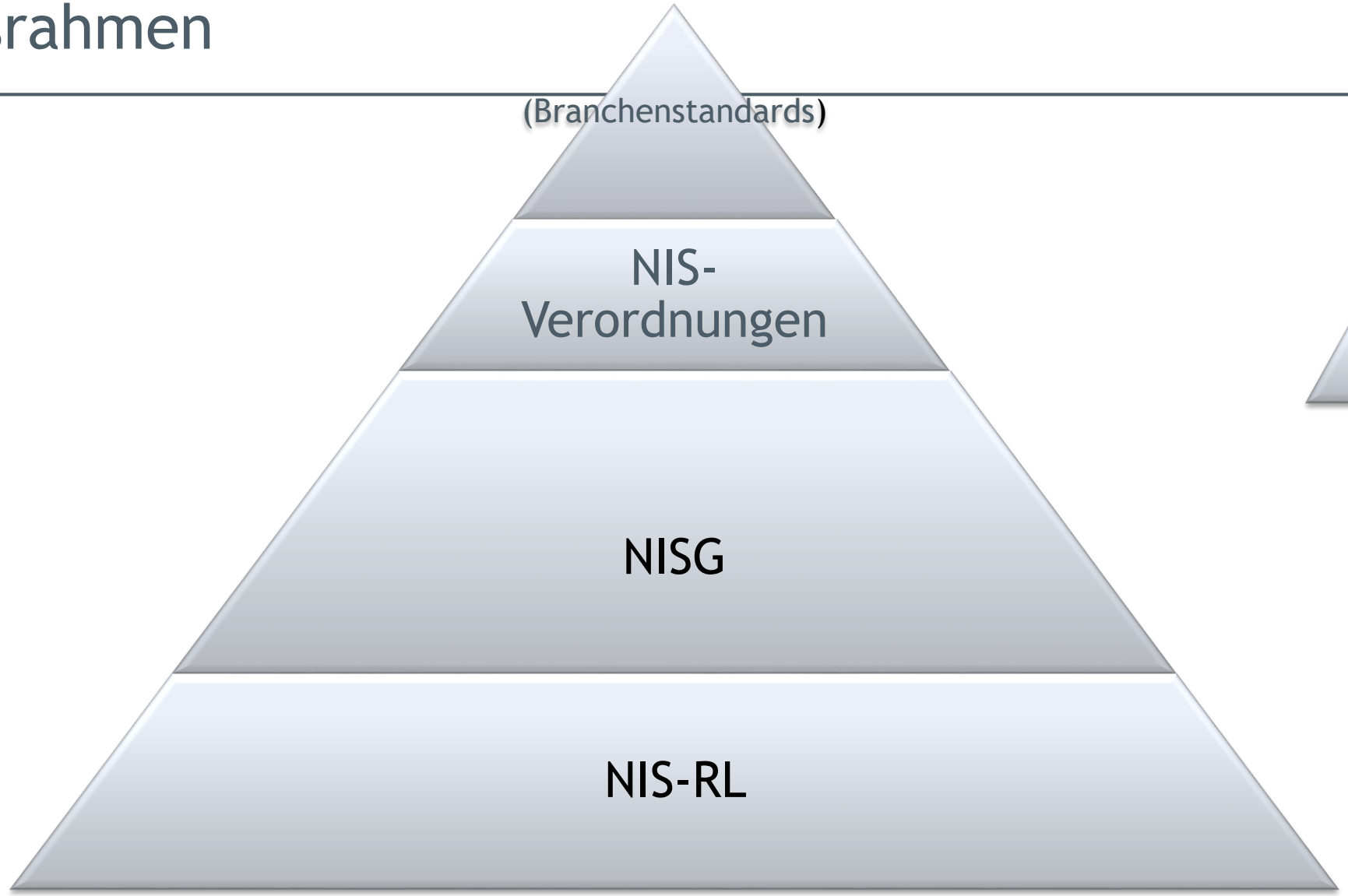
Netz- und Informationssicherheit

§ 3 Z 2 NISG



DSGVO: Schutz personenbezogener Daten

Rechtsrahmen



NIS-Richtlinie - Allgemeines

© Rawpixel_Shutterstock_com

- Richtlinie 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

- erste EU-weite Regelung zu Cybersicherheit

- Ziel: hohes Sicherheitsniveau der Netz- und Informationssysteme

NIS-Richtlinie - Inhalt

©Fotolia

- Zusammenarbeit der Mitgliedstaaten
- nationale NIS-Strategien
- Sicherheitsvorkehrungen und Meldepflichten für
  - Betreiber wesentlicher Dienste
  - Anbieter digitaler Dienste
  - nicht: öffentliche Verwaltung

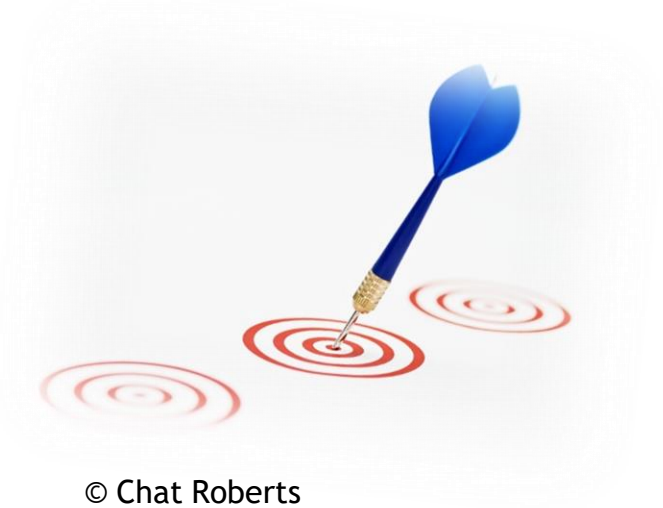
DSGVO: alle

NISG – Inhalt I

- Einrichtung nationaler Organisations- und Koordinationsstrukturen
  - Bundeskanzler: strategische Aufgaben
  - BMI: operative Aufgaben
  - BMLVS: operativ (Defense)
- nationale NIS-Strategie
- Computer-Notfallteams (CSIRTs oder auch CERTs)

NISG – Inhalt II

- Adressaten
  - Betreiber wesentlicher Dienste
  - Anbieter digitaler Dienste
  - Einrichtungen des Bundes
  - qualifizierte Stellen zur Überprüfung
- Verpflichtungen
- Sanktionen



© Chat Roberts

Betreiber wesentlicher Dienste

Pflichten für Betreiber wesentlicher Dienste

- geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen
- unverzügliche Meldung von Sicherheitsvorfällen
- Ausnahme: sektorenspezifische EU-Vorschriften
- freiwillige Meldung

DSGVO: geeignete technische und organisator. Maßnahmen Meldepflichten

Sicherheitsvorkehrungen – Mindestsicherheitsmaßnahmen

- „Mapping-Tabelle“ =

Mindestsicherheitsmaßnahmen mit nationalen und internationalen **IKT-Sicherheitsstandards** und **Cyber Security Best Practices**

- öst. Informationssicherheitshandbuch (Version 4.0.1)
- BSI IT-Grundschutz
- ISO 27001:2013
- ISA/IEC 62443 3-3
- CIS Critical Security Controls 6.0 und 7.0
- NIST Cyber Security Framework

Überprüfung von Betreibern wesentlicher Dienste

- Nachweis mind. alle 3 Jahre
  - Zertifizierungen oder
  - Überprüfungen durch qualifizierte Stellen
- Überprüfung durch BMI jederzeit
- BMI kann Empfehlungen aussprechen

© Corbis

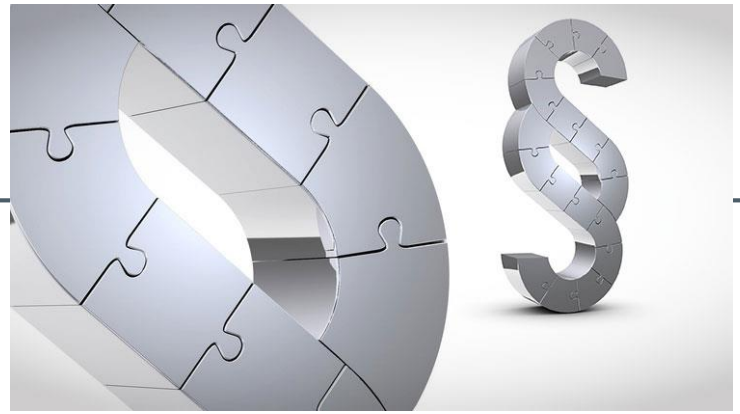
Anbieter digitaler Dienste

© Fotolia

- Juristische Person:
  - Online Marktplatz
  - Online Suchmaschine
  - Cloud Computing-Dienst
- NICHT:
  - Klein- und Kleinstunternehmen:

    < 50 Mitarbeiter UND Jahresumsatz/bilanz < 10 Mio. EUR
- Vollharmonisierung:
  - keine Ermittlung durch MS
  - Durchführungsverordnung (EU) 2018/151

Pflichten für Anbieter digitaler Dienste



© Fotolia

- geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen
- unverzügliche Meldung von Sicherheitsvorfällen wenn
  - Zugang zu Informationen, die benötigt werden um die Auswirkung eines Sicherheitsvorfalls zu bewerten
- freiwillige Meldung
- Überprüfung durch BMI nur im Anlassfall
- BMI kann Empfehlungen aussprechen

Sicherheitsvorfall

© Josef Schauer-Schmidinger/WKO Inhouse GmbH

- Störung
  - der Verfügbarkeit
  - Integrität
  - Authentizität oder
  - Vertraulichkeit von Netz- und Informationssystemen
- Ausfall oder Einschränkung der Verfügbarkeit des Dienstes
- mit erheblichen Auswirkungen
  - betroffene Nutzer, Dauer, geografische Ausbreitung, Auswirkung auf Wirtschaft und Gesellschaft

Sanktionen

- Verwaltungsstrafe bei Verstoß gegen Vorgaben NISG
  - Meldepflicht
  - Sicherheitsvorkehrungen
  - Mitwirkungspflichten
- bis EUR 50.000
- Wiederholungsfall bis EUR 100.000
- auch gegen juristische Person möglich

- zuständig: Bezirksverwaltungsbehörde

© Moment/cultura/Corbis

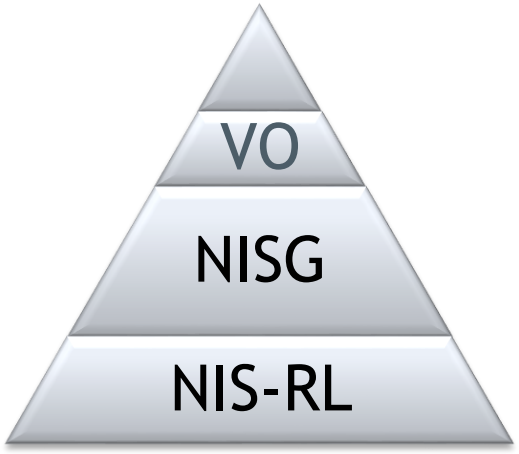
Verstoß gegen Art. 32 DSGVO: bis EUR 10 Mio. oder 2% Jahresumsatz

und jetzt...???

WKÖ Bilderpool

Zusammenfassung

- Sicherheit von Netz- und Informationssystemen
- betroffen:
  - Betreiber wesentlicher Dienste (kritische Infrastrukturen)
  - Anbieter digitaler Dienste
  - öffentliche Verwaltung
- Sicherheitsvorkehrungen
- Meldepflichten bei Sicherheitsvorfällen



Links

- NIS-Gesetz und Erläuterungen
- NIS-Richtlinie
- Europäische Cybersicherheitsstrategie
- Österreichische Cybersicherheitsstrategie
- Bericht Cybersicherheit 2018
- www.it-safe.at

Vielen Dank für Ihre Aufmerksamkeit.