Das neue NIS-Gesetz: Schutz der IT hinter den kritischen Infrastrukturen

Otmar Lendl
<lendl@cert.at>

Vorstellung

- Mag. Otmar Lendl
  - Uni Salzburg, ISPs (Ping, EUnet, KPNQwest), nic.at R&D
  - Seit 2008 Teamleiter von CERT.at
- Nationales CERT für Österreich
  - Computer Emergency Response Team
  - nic.at in Kooperation mit dem Bundeskanzleramt

CERT.at

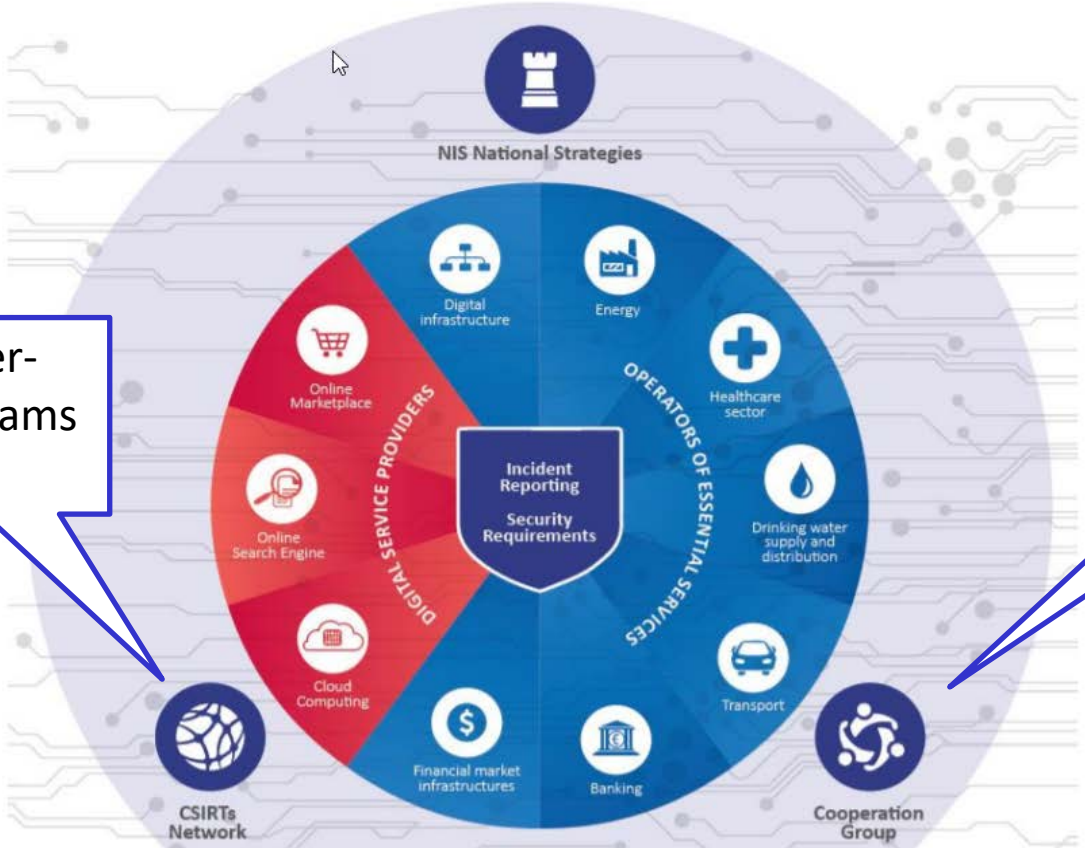
- Nationales CERT für Österreich
  - „CERT of last resort“ (Subsidiaritätsprinzip)
- Aufgaben
  1. **Informationen**: Warnungen, Tageszusammenfassungen, Pressearbeit
  2. **Netzwerk Hygiene**: Was läuft alles schief in Österreich -> Information der Betroffenen
  3. **Reaktiv**: Hilfe bei Vorfällen
  4. **Networking**: Community-Building, Trust Circle, CERT-Verbund, CSIRTs Network

NIS Richtlinie?

- **Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union**
- Richtlinie, nicht Verordnung
- **“Minimum-Harmonisierung”**
  - MS dürfen - abweichend von den Regelungen in der Richtlinie - Bestimmungen erlassen, die ein höheres Sicherheitsniveau von Netzen und Informations-systemen ermöglichen
  - Bestimmte Bereiche sind von dieser Regelung aber explizit ausgenommen

NIS-RL in a nutshell

- Identifikation wesentlicher Dienstleistungen / Betreiber
  - Mindeststandards für IT Sicherheit
  - Meldepflicht bei Vorfällen (+ Melderecht)
- National Etablierung von
  - CSIRTs (CERTs)
  - Zuständigen Behörden
- Kooperation in der EU
  - CSIRT Netzwerk
  - Kooperationsgruppe
- Verpflichtung zur Festlegung einer nationalen NIS-Strategie



Computer-Notfallteams (CSIRTs)

Nationale zuständige Behörde(n)

Timeline

- EU:
  - Beschluss: 6. Juli 2016
  - Inkrafttreten: 8. August 2016
  - Danach laufend diverse Implementierungsschritte
- Nationale Umsetzung:
  - Deadline war 9. Mai 2018
  - Gesetz kam Ende 2018
  - Verordnungen RSN
  - Bescheide in den nächsten Wochen

Links

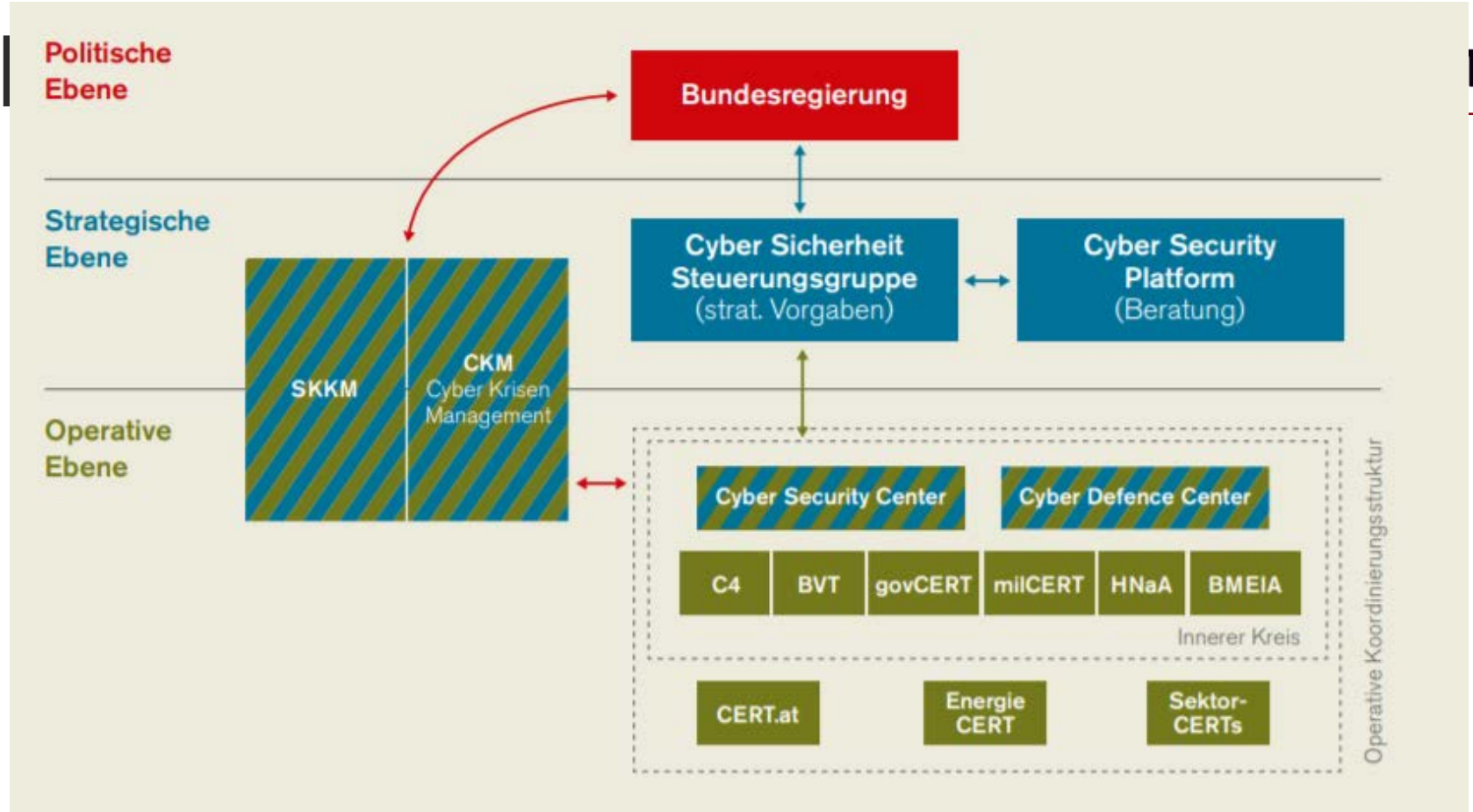
- https://www.nis.gv.at/ wird das nationale Portal zu diesem Thema
- https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive (leider nicht aktuell)
- https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
- https://csirts-network.eu/

NIS Behörden

- Strategische
  - Im BKA
    - Sicherheitsvorgaben
    - Cooperation Group
- Operative
  - Im BM.I (Cyber Security Center im BVT)
    - Aufsicht bzgl. Sicherheitsvorgaben
    - Lagebild
    - Krisenprozesse

ÖSCS Umsetzung

- Österreichs Strategie für Cyber Sicherheit
- Vieles, was in der ÖSCS (2013) beschrieben wurde, wird mit dem Gesetz verankert
- Inbesondere die Strukturen
  - CSC
  - IKDOK
  - OpKoord


Politische Ebene
Bundesregierung
Strategische Ebene
Cyber Sicherheit Steuerungsgruppe (strat. Vorgaben)
Cyber Security Platform (Beratung)
SKKM
CKM Cyber Krisen Management
Operative Ebene
Cyber Security Center
Cyber Defence Center
C4
BVT
govCERT
milCERT
HNaA
BMEIA
Innerer Kreis
CERT.at
Energie CERT
Sektor-CERTs
Operative Koordinierungsstruktur

CSIRTs

- Wunsch: Selbstorganisation in den Branchen
  - Sektorale CSIRTs
  - Austrian Energy CERT
  - GovCERT
- CERT.at als „Nationales Computer-Notfallteam“

Betreiber wesent. Dienste

- Sie werden per Bescheid zu solchen
- Müssen Kontaktestellen melden
- Sicherheitsvorkehrungen
- Meldepflichten
  - unverzügliche Meldung eines Sicherheitsvorfalls beim zuständigen Computer-Notfallteam (CSIRT)
  - freiwillige Meldungen

Sicherheitsvorkehrungen

- Standards
  - geeignet, um hohes Sicherheitsniveau von NIS zu gewährleisten
  - dem Stand der Technik entsprechend
  - technisch und organisatorisch
  - Aufbauend auf existierende Standards
  - Nicht nur gegen böswillige Angriffe
- Qualifizierte Stellen zur Überprüfung
  - Alle 3 Jahre alle Kapitel
  - Kann in Teilen gemacht werden

Vorfallsmeldungen

- Pflichtmeldungen
  - Unverzüglich an das CSIRT
  - Weitergabe an BM.I
- Freiwillige Meldungen
  - An CSIRT möglich
  - Auf Wunsch anonym
  - Sammelmeldung an BM.I
- Warum so komplex?
  - Trennung Helfer / Aufsicht

WO WIR NICHT HINWOLLEN:

„Der Pathologe weiß alles ganz genau …
aber leider zu spät“

Melderechte

- Staatliche Meldepflichten sind kein Ersatz für freiwillige Kooperation
- Freiwilliger Informationsaustausch MUSS zwischen den (potentiell) Betroffenen möglich sein
  - zeitnah und umfassend
  - auch abseits von Meldepflichten – z.B. Schwellwerten
  - auf Wunsch anonymisiert
  - auf einer gesicherten rechtlichen Basis
  - Ohne, dass sofort Ermittlungsverfahren gegen den Willen der Betroffenen eingeleitet werden

Fazit

- IT ist für unsere Gesellschaft essentiell
  - Der Staat kontrolliert nicht die Infrastruktur
  - Er kann nur die Betreiber zu guter Arbeit anhalten
- Das NISG betrifft die wesentlichen Dienste
  - KMUs sind im Normalfall **nicht** betroffen
- nic.at spielt mit CERT.at in der NIS Umsetzung eine wichtige Rolle, Serviceangebot an die Wirtschaft

Fragen?

Otmar Lendl <lendl@cert.at>