Eine AT Strategie für Netzsicherheit

mit Schwerpunkt auf europäischen Entwicklungen zu 5G-Sicherheit

Mag. Vinzenz Heußler, LL.M. Mag. Arno Spiegel

BKA, Abt I/C/8 – Cyber Security, GovCERT, NIS-Büro und ZAS

Salzburg, 05.09.2022

Übersicht

- Ausganslage
- Strukturen
- Rechtlicher Rahmen
- Österreichische Strategie für Cybersicherheit (ÖSCS 2021)

Ausgangslage

- Anhaltend steigende Computerkriminalität
- Zunehmende Verflechtung kritischer Infrastrukturen mit dem Internet
- Permanent wachsende Abhängigkeit von Staat, Wirtschaft und Gesellschaft von einer funktionierenden IKT

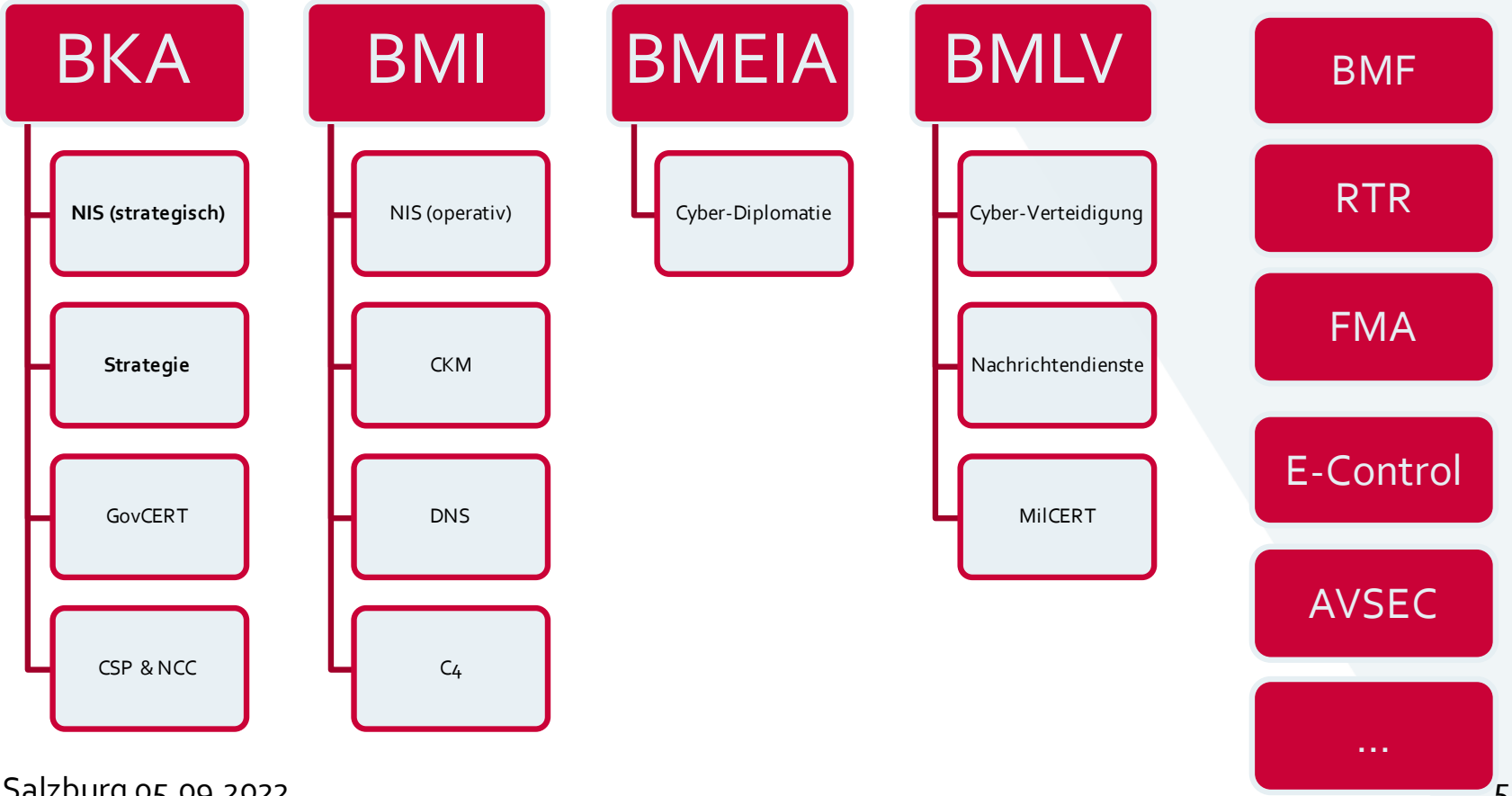
→ **Cybersicherheit** wird von einem individuellen Problem **zu einer sicherheits-politischen Herausforderung** mit gesamtgesellschaftlicher Dimension

→ Umfassende Maßnahmen zur **Erhöhung der Resilienz** notwendig

→ Basis sind die **AT-Strategie** und die **EU-Strategie** für Cybersicherheit

Strukturen

- Staatlichen Kompetenzen in Österreich **stark fragmentiert** (Querschnittsmaterie)
  - Schutz und Prävention gegenüber Angriffen auf IKT auf mehrere Ressorts (und Regulatoren) aufgeteilt
  - Keine Einrichtung alleine kann verbindliche Vorgaben machen
  - Starke und effektive Koordinierung und Bündelung der Kräfte notwendig
  - Zusammenarbeit und Schaffung von Synergien wird in Teilbereichen gelebt
  - Informationsaustausch notwendig
  - Gesetzliche und organisatorische Rahmenbedingungen wirken einschränkend.


BKA
NIS (strategisch)
Strategie
GovCERT
CSP & NCC
BMI
NIS (operativ)
CKM
DNS
C4
BMEIA
Cyber-Diplomatie
BMLV
Cyber-Verteidigung
Nachrichtendienste
MilCERT
BMF
RTR
FMA
E-Control
AVSEC
...

Rechtlicher Rahmen

- Netz- und Informationssystemsicherheitsgesetz (NISG)
  - Setzt die Richtlinie (EU) 2016/1148 vom 6. Juli 2016 (NIS-RL) um
- Definiert Strukturen, Aufgaben, Behörden, CSIRTs, Strategie etc.
- Verpflichtet Einrichtungen mit hoher Bedeutung für das Gemeinwesen, Sicherheitsvorkehrungen einzurichten und Sicherheitsvorfälle zu melden
- EU-Rechtsakte:
  - NIS1, EECC, CSA, ECCC
  - NIS2, DORA, CRA, Aviation Safety, Network Code in Electricity, RED,…

Österreichische Strategie für Cybersicherheit (ÖSCS 2021)

- 4 Herausforderungen
- 1 Vision
- 12 Ziele
- 4 Zielgruppen
- 4 Chancen
- Monitoring

- Maßnahmenkatalog

ÖSCS – Herausforderungen

- Bedrohungen, die das Ergebnis der missbräuchlichen Nutzung von IT sind
- Bedrohungen, die das Ergebnis von falscher Nutzung der IT sind
- Bedrohungen, die das Ergebnis der Abhängigkeit von IT sind
- Bedrohungen durch neue Technologien

ÖSCS – Vision

- Langfristige Schaffung eines sicheren Cyberraumes als Beitrag zur Steigerung der Resilienz Österreichs und der EU durch einen gesamtstaatlichen Ansatz. Um diese
- Zur Verwirklichung der Vision verfolgt die ÖSCS 12 Ziele
- Europäischer Ansatz:
  - Jegliche Stärkung der Cybersicherheit der EU ist auch eine Stärkung der österreichischen Cybersicherheit.
  - Österreich bekennt sich daher zur Förderung und Umsetzung der Cybersicherheitsstrategie der EU

ÖSCS – Ziele

1. **Ressourcenallokation:** … ausreichende finanzielle und personelle Ressourcen … … um Cyberbedrohungen und -vorfällen vorzubeugen
2. **Fähigkeitenentwicklung:** … Fähigkeit … kritischen Informationssysteme und Infrastrukturen zu schützen
3. **Gemeinschaftliche Aufgabe**: Gesellschaft, Wirtschaft und Staat; Verantwortlichkeiten und Zuständigkeiten klar geregelt
4. **Gesamtstaatliches Lagebild** und **Cybersicherheitskompetenzen**: in allen Gesellschafts-, Lebens- und Berufsbereichen (Awarness)
5. **Partizipation**: Sichere am gesellschaftlichen und politischen Leben im Cyberraum teilhaben

ÖSCS – Ziele

6. **Klare** gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten … ggf adäquate Strafverfolgung
7. **Aktives Engagement**: Stakeholder auf nationaler, europäischer und internationaler Ebene
8. **Digitale Souveränität**: im Zusammenwirken mit der EU
9. **Forschungs- und Entwicklungslandschaft**: koordiniert und vernetzt
10. **Fachkräfte**: Ausbildung, Nachfrage des Arbeitsmarktes erfüllen

ÖSCS – Ziele

11. **Diplomatie**: aktiver Beitrag bei der Anwendung und Stärkung internationaler Normen

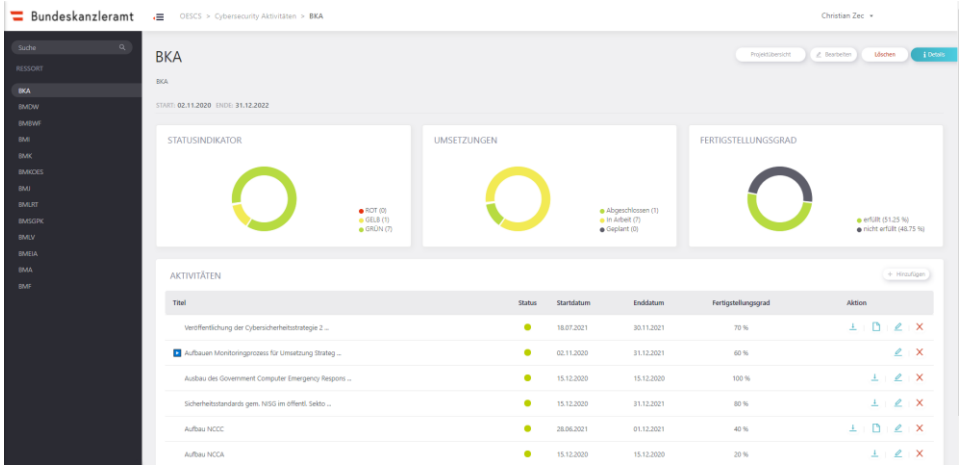
12. **Gesamtstaatlicher Ansatz**: Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität.

ÖSCS – Zielgruppen

- Gesellschaft
- Wirtschaft
- Bildung, Forschung und Entwicklung
- Öffentlicher Sektor

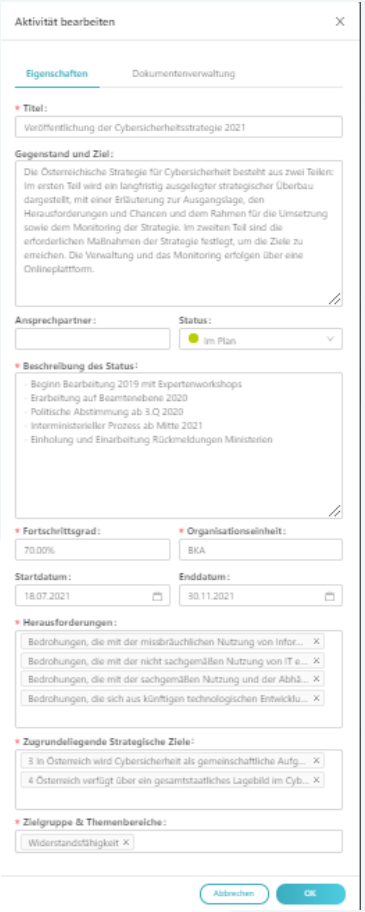
ÖSCS – Maßnahmenkatalog

- Webseitengestützter Maßnahmenkatalog mit Monitoring und Auswertung
  - Agiles Reagieren auf technologische Entwicklungen
  - Erlaubt automationsgestützte Auswertungen und Fortschrittsmessung



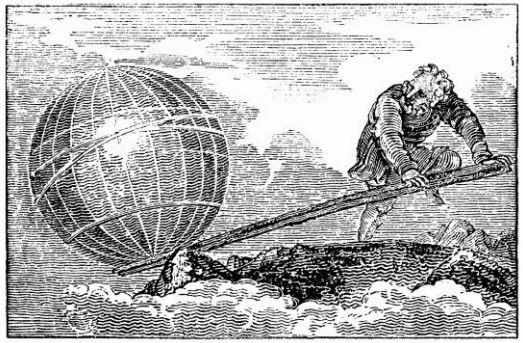
ÖSCS – Maßnahmenkatalog

- Durch Stakeholder selbst definiert und gepflegt
- Maßnahmenbezug zu Zielen, Zielgruppen und Themenbereich
- Interministerielle Maßnahmenkoordination
- Fortschrittsmessung und Qualitätsmanagement



ÖSCS – Hebelwirkung

- Maßnahmen werden auf Vorschlag der CSS vom Ressort-GS (bzw. Konferenz der GS) beauftragt
- Im Rahmen Umsetzungsbeauftragung durch den Generalsekretär erfolgt insb auch die Sicherstellung organisatorischer, finanzieller und technischer Voraussetzungen
- Umsetzung federführend durch Ressort-CISOs
- Maßnahmen aus dem Privatsektor durch CSP oder NCC
- Regelmäßiger Fortschrittsbericht, wird (wo nicht sicherheitskritisch) veröffentlicht



Cybersecurity in 5G

Mag. Arno Spiegel
Abteilung I/C/8 – Cyber Security, GovCERT, NIS-Office und ZAS
Salzburg, 05.09.2022

Einleitung

- Rückblick
- Cybersecurity of 5G EU Toolbox
  - Inhalt
  - nationale Umsetzung
- Ausblick

März 2019: Empfehlung der Kommission


EUROPEAN COMMISSION

Strasbourg, 26.3.2019
C(2019) 2335 final

COMMISSION RECOMMENDATION

of 26.3.2019

Cybersecurity of 5G networks

EN EN

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154

zur Cybersicherheit von 5G Netzen mit den Zielen:

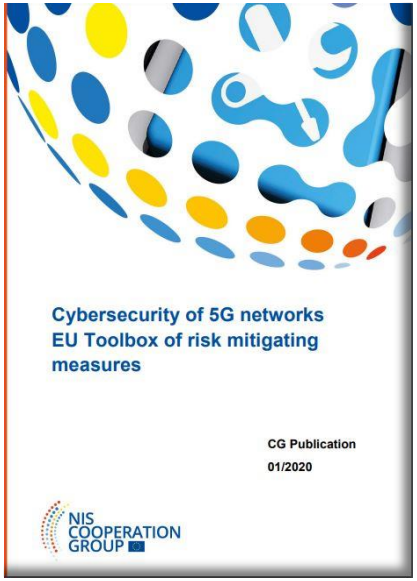
- Durchführung einer nationalen Risikoanalyse mit Fokus auf 5G Netzwerke bzw. Aktualisierung bestehender nationaler Risikoanalysen
- Verbesserung der Kooperation auf EU-Level und Durchführung einer EU-weiten Risikoanalyse
- Vorschlag der Schaffung einer Toolbox um den analysierten Risiken zu begegnen

9. Oktober 2019: EU coordinated risk assessment

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

- Überprüfung der unionsweiten Risikoexposition der Mitgliedstaaten zu:
  - Bedrohungen und Akteure
  - Assets
  - Schwachstellen
  - Risikoszenarien
- Besondere Rolle der NIS – Kooperationsgruppe bzw. des eigens geschaffenen Work-Streams

29. Jänner 2020: EU Toolbox - 1



https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

- Toolbox: Identifikation von Risiken die mit 5G Netzen verbunden sind (basierend auf der europäischen Risikoanalyse) und mögliche Abhilfemaßnahmen (mitigation measures):
  - strategisch
  - technisch
  - unterstützend

EU Toolbox – 2: 8 strategische Maßnahmen (Auszug)

- Stärkung der Rolle der nationalen Behörden
- Durchführung von Sicherheitsaudits bei den Betreibern
- Erstellung von Risikoprofilen der Hersteller, einschließlich der Möglichkeit, Beschränkungen oder Ausschluss eines Lieferanten mit hohem Risiko zu ermöglichen
- Förderung von Strategien mit mehreren Anbietern, um Abhängigkeiten zu vermeiden (Multi-Vendor)
- Stärkung der Widerstandsfähigkeit auf nationaler Ebene

EU Toolbox – 3: 11 technische Maßnahmen (Auszug)

- Sicherstellung der Anwendung grundlegender Sicherheitsanforderungen bei der Netzgestaltung und –architektur
- Evaluierung der Anwendung von 5G-Sicherheitsstandards auf MNOs (Mobile Network Operators)
- Erhöhte Sicherheit für virtualisierte Netzwerkfunktionen
- Sicherheit für 5G-Netzmanagement, -betrieb und –überwachung
- EU-Zertifizierung für 5G-Netzkomponenten, Kundengeräte, Prozesse bei Herstellern und für weitere Nicht-5G-Komponenten und -Dienste

EU Toolbox – 4: 10 Unterstützungsmaßnahmen (Auszug)

- Überarbeitung oder Entwicklung von Leitfäden und bewährten Verfahren (best practices) zur Netzsicherheit
- Stärkung des Potenzials für Tests und Audits auf nationaler und EU-Ebene
- Entwicklung und Unterstützung der 5G-Standardisierung
- Gewährleistung von technischen und organisatorischen Sicherheitsmaßnahmen durch ein spezielles EU-weites Zertifizierungssystem
- Analyse der Interdependenzen zwischen 5G-Netzen und anderen kritischen Diensten

Umsetzung der Toolbox 1

- Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020) der RTR, normiert Informationspflichten, Mindestsicherheitsmaßnahmen und den Nachweis von Informationssicherheitsmaßnahmen für 5G Netze mit mehr als 100.000 Teilnehmern.
  - technisch
- TKG 2021: §44 „Sicherheit und Integrität", setzt die Meldeverpflichtungen nach EECC und NISG um
  - technisch

Umsetzung der Toolbox 2

- TKG 2021: §45 „Hochrisikolieferanten", Einstufung als solcher durch den zuständigen Bundesminister bei Mängel der Produkte, mangelnde Sicherheits- und Datenschutzübereinkommen oder Unvermögen einer der durchgängigen Versorgung.
  Vor der Entscheidung: Befassung des Fachbeirat für die Sicherheit in elektronischen Kommunikationsnetzen.
  - technisch und „politisch"

Ausblick

- 5G Zertifizierungsschema
- Cyber Resilience Act (CRA)
- State of the Union – Rede 14.09.2022?

Vielen Dank für die Aufmerksamkeit!

Abteilung I/C/8 – Cyber Security, GovCERT, NIS-Office und ZAS
nis@bka.gv.at