

Europäische Cybersicherheits-Initiativen und Umsetzung in Österreich *)

Herbert.Leitold@a-sit.at

23. ISSS Berner Tagung für
Informationssicherheit

Online, 18.11.2020

*) *Folien teilweise dankenswerter Weise vom Bundeskanzleramt Österreich*

Über mich

- Generalsekretär A-SIT
- Vor allem in eID, elektronischer Signatur und eGovernment tätig
- öst. Mitglied in eIDAS Experten-
gruppe, Kooperationsnetzwerk
und stv. Mitglied ENISA Verwaltungsrat



Inhalte



- eIDAS und Review
- NIS und Review
- Cyber Security Act
- NCCC
- CyCLONe
- DORA
- Joint Cyber Unit



- E-ID „neu“
- Prüfung Betreiber w.D.
- gesetzl. Umsetzung

*Aktuelle Entwicklungen,
noch nicht final definiert*

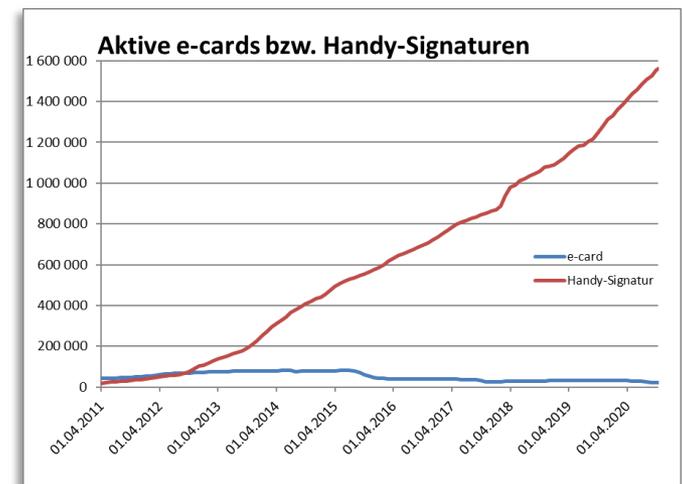


- EU Verordnung eID und Vertrauensdienste
 - Vertrauensdienste seit Juli 2016 in Kraft
 - dzt. 236 Anbieter qualifizierter Vertrauensdienste
 - z.B 153 qual. Signaturzert., 106 qu. Siegel, 20 el. Einschreiben
 - Bisher 19 eID Schemen aus 16 MS notifiziert
- eIDAS Review im Laufen
 - Mitteilung Europäische Kommission Ende 2020 erwartet
 - u.a. „EUid“, z.B. Europäischer Rat am 2. Oktober 2020
„Er [der Rat] ersucht die Kommission, bis Mitte 2021 einen Vorschlag für eine Initiative zur „europäischen digitalen Identifizierung“ vorzulegen.“

eIDAS in Österreich



- Signatur und eID zentral im österr. eGovernment
 - Umgesetzt über Bürgerkarte und Handy-Signatur
 - dzt. 1,6 Mio. NutzerInnen, ca. 1,8 Mio. Nutzungen p.m.
 - auch alle Ausfertigungen einer Behörde elektr. signiert
- Eigenschaften österreichische eID
 - technologieneutral mit Karte und mobiler eID seit 2005/10
 - Identifikation, qualif. Signatur und elektronische Vertretung
 - Nur mobile Lösung erfolgreich



E-ID neu ab 2021



- Überarbeitung aus bisheriger Erfahrung, aus eIDAS und aus Strategie „mobile-first“
 - Nur mehr mobile Lösung mit Fernsignatur
 - Erweiterung um weitere Attribute / Attributanbieter
 - Integration in mobiler App „Digitales Amt“
 - Nur mehr behördliche Registrierung
- Aktuell Pilotierung, Produktivsetzung in 2021

NIS Richtlinie

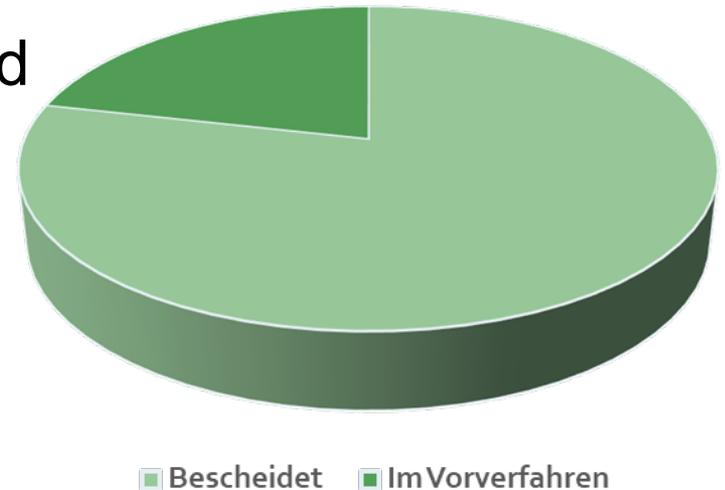


- 2016 verabschiedet
 - Regelt Sicherheitsanforderungen an Betreiber wesentlicher Dienste (Energie, Verkehr,)
- Evaluierung der NIS-RL bis 9.5.2021
 - EU-Kommission hat sich selbst das Ziel Q4/2020 in ihrem Arbeitsprogramm gesetzt
 - <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-%20%20Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems>
 - Im Q4 sollen von der EK veröffentlicht werden:
 - Evaluierungsbericht und Textvorschlag zu „NIS RL2“
 - neuer Textvorschlag für Bereich Schutz kritischer Infrastruktur
 - die Cybersicherheitsstrategie der EU

NIS Richtlinie in Österreich (I/II)



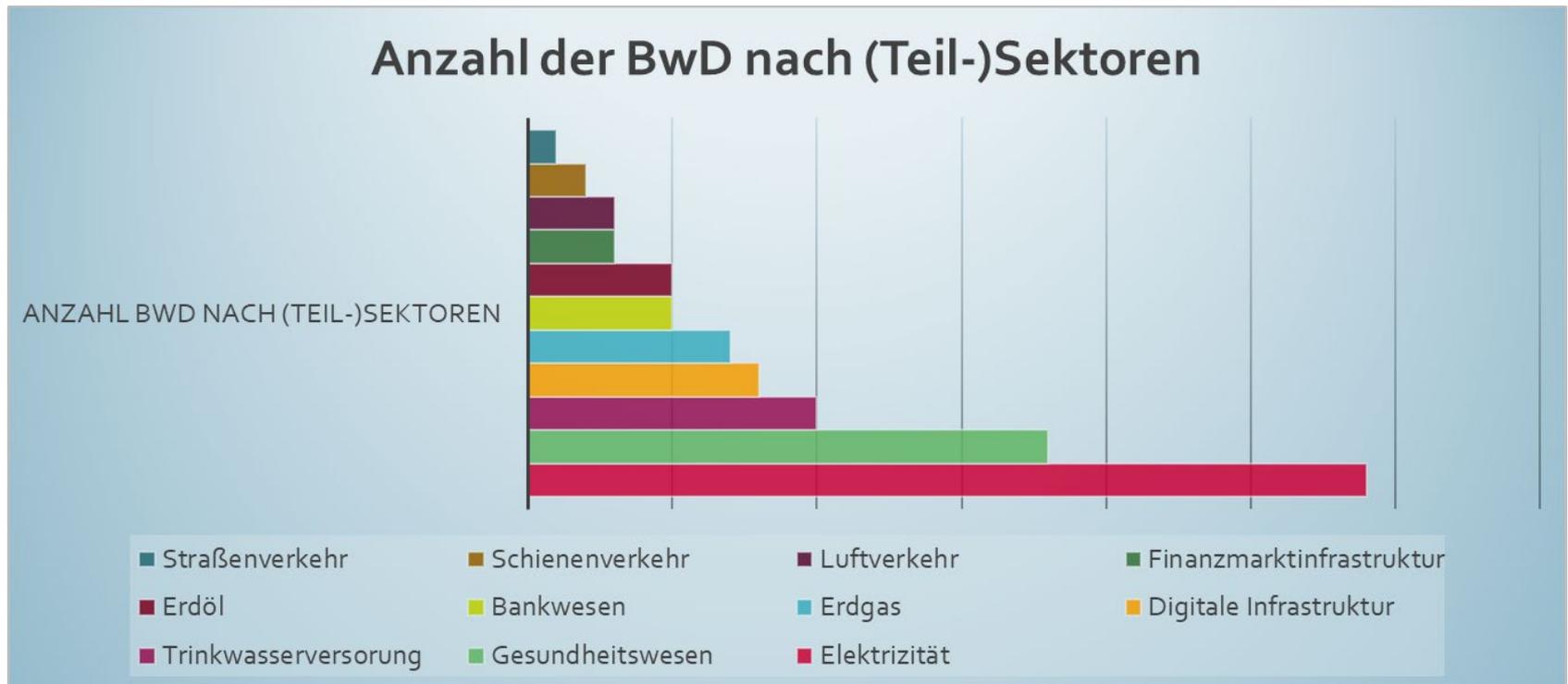
- NIS Gesetz 2018, NIS Verordnung 2019
 - 2019 als Computer-Notfallteam CERT.AT festgestellt
 - Austrian Energy CERT (AEC) seit 06/2020
- Betreiber wesentlicher Dienste
 - werden behördlich ermittelt und per Bescheid festgestellt
 - Erfüllung Anforderungen mindestens alle 3 Jahre
 - Meldepflicht von Vorfällen



NIS Richtlinie in Österreich (II/II)



- Verteilung Betreiber wesentlicher Dienste



Cyber Security Act



- Seit 2019 in Kraft
- Permanentes Mandat für ENISA
- Zertifizierungs-Infrastruktur
 - ECCG und SCCG eingerichtet
 - EU Schemen ersetzen nationale Schemen
 - EUCC Candidate Scheme veröffentlicht
<https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme>
 - Wird SOG-IS ersetzen
 - Umsetzungsrechtsakt noch ausständig
 - 5G Schema in Diskussion
 - Cloud Schema in Arbeit

Cyber Security Act in Österreich



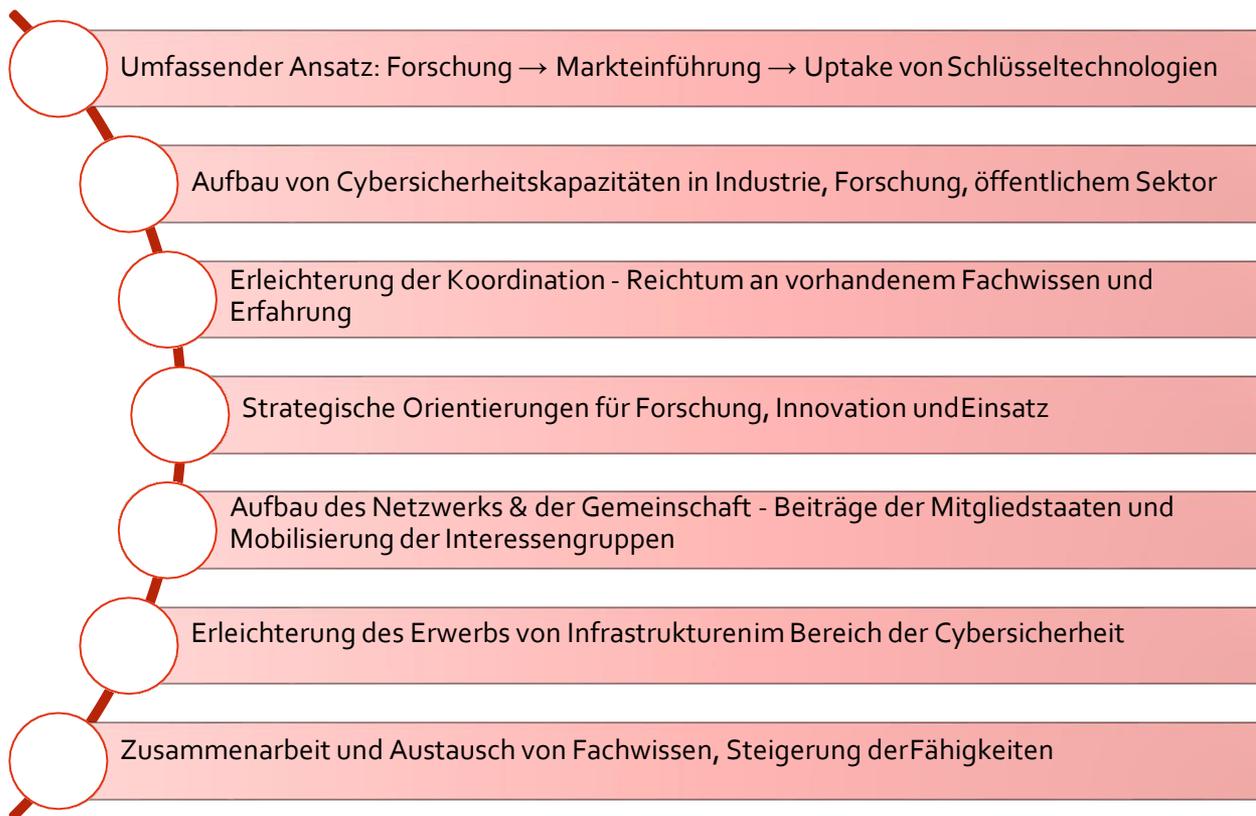
- Gesetzliche Umsetzung zu den Teilen Zertifizierung noch nicht abgeschlossen
- Österreich Mitglied in CC-MRA und SOG-IS
 - bisher konsumierend (nicht zertifizierend)
 - daraus kein unmittelbarer Handlungsdruck
- Mit SGS mittlerweile CC Prüfstelle in Ö

NCCC (I/III)



- Einrichtung Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren
- Vorschlag für eine EU-Verordnung, vorgelegt am 12. September 2018, seither in Verhandlung
<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018PC0630>
https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=consil:ST_14368_2018_REV_1
[https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2018/0328\(COD\)](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2018/0328(COD))
- Soll die Cybersicherheitsaspekte diverser Programme (insb. des Digitale Europe Programme, Horizon Europe Programme, Next Generation EU) implementieren

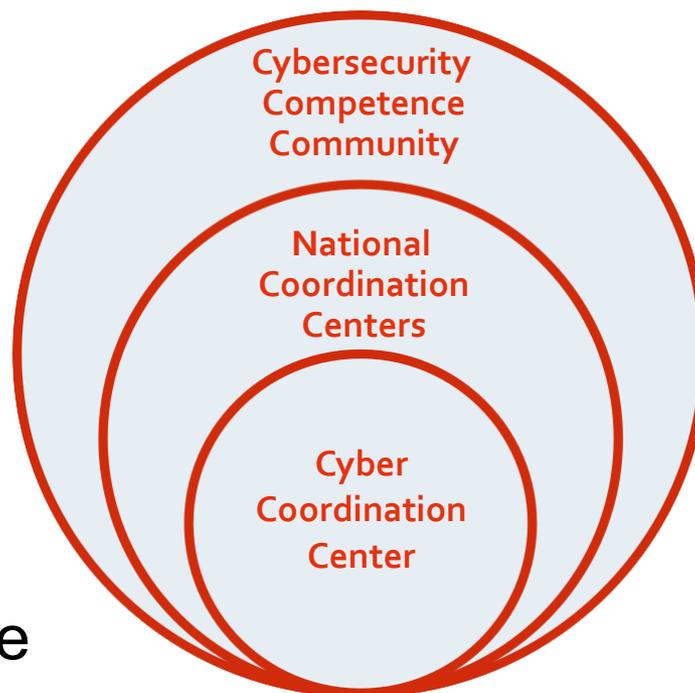
NCCC (II/III)



NCCC (III/III)



- Cybersecurity Competence Community
- National Coordination Centre
- European Cybersecurity Industrial, Technology and Research Competence Centre



CyCLONe (I/II)



- 2017: Empfehlung der EU-Kommission „für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen“ (Blueprint) <https://eur-lex.europa.eu/eli/reco/2017/1584/oj>
 - In NIS-KG beschäftigte sich Work Stream 7 mit der Implementierung des Blueprint
 - Aktueller Status und Funktionsweise NIS-SPOC erweist sich als bedingt effizient und nutzbar
- **CyCLONe: Cyber Crises Liaison Organisation Network**
 - Eine effiziente Vorgehensweise bei großflächigen Cybersicherheitsvorfällen und -krisen in der EU
 - Etablierung eines Netzwerkes zur Kooperation zuständiger nationaler Behörden bei Cybervorfällen und -krisen

CyCLONe (II/II)



- Operative Verknüpfung zw. politischer und technischer Ebene
 - Politisch: Rat der EU (Krisenreaktionsmechanismus der EU; Integrated Political Crisis Response IPCR)
 - Technisch: CSIRTs-Netzwerk (Netzwerk der nationalen Computer Notfallteams auf EU-Ebene)
- Aufgaben (u.a.)
 - Erstellung von Lagebildern
 - Koordination des Krisenmanagements
 - Unterstützung für politische Entscheidungen
 - Vorlagen und Tools zur Kommunikation

DORA



- Digital Finance Package
https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en
- Legislativvorschläge „Digital Operationale Resilience Act – DORA“
<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020PC0595>
- Soll sicherstellen, dass alle Teilnehmer des Finanzsystems über die notwendigen Sicherheitsvorkehrungen verfügen, um Cyber-Angriffe und andere Risiken einzudämmen
- Sehr weiter Anwendungsbereich (Ausnahme Kleinstunternehmen)

Joint Cyber Unit, gemeinsame Cyber-Stelle



- Arbeitsprogramm Präsidentin der EU-Kommission
https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_de.pdf
- Bestätigt in Sicherheitsstrategie der EU Juli 2020
<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605>

„... dass eine gemeinsame Cyber-Stelle für eine strukturierte und koordinierte operative Zusammenarbeit erforderlich ist. Diese könnte auch einen Amtshilfemechanismus auf EU-Ebene für Krisenzeiten umfassen. [...] Vertrauen zwischen den verschiedenen Akteuren im europäischen Cybersicherheitsgefüge aufgebaut und den Mitgliedstaaten ein wichtiger Dienst angeboten werden. [...] bis Ende 2020 ein klares Verfahren, Etappenziele und eine Zeitplanung festlegen“

Ich danke für Ihre
Aufmerksamkeit!



Herbert.Leitold@a-sit.at