IT-SICHERHEITSGESETZ 2.0 – QUO VADIS? WAS ERWARTET UNS 2021?

Boban Krsic, CISO
verinice.XP, 25.02.2021

BOBAN KRSIC

EXPERIENCE

- 2011 – present: DENIC eG, Frankfurt/Main, Germany, Chief Information Security Officer (CISO)
- 2010 – present: DACONIS GmbH, Frankfurt/Main, Germany, Founder and CEO
- 2007 – 2011: Steria Mummert Consulting, Hamburg, Germany, Senior Security Consultant
- 2006 – 2007: AREVA Nuclear Power, Offenbach, Germany, Strategic Product Management

PROFESSIONAL DEVELOPMENT - CERTIFICATIONS

- Certified Cloud Security Professional; ISC^2 (2019)
- Agile Certified Practitioner; PMI (2014)
- ISO 22301 Lead Auditor; BSI (2012)
- Certified in Risk and IS Control; ISACA (2011)
- Certified Information Security Manager; ISACA (2010)
- COBIT Practitioner; ISACA (2010)
- ISO/IEC 27001 Lead Auditor; BSI (2010)
- Certified Information Systems Auditor; ISACA (2009)
- Certified IS Security Professional; (ISC)^2 (2008)
- ISO 27001-Auditor - Basis von IT-Grundschutz; BSI (2007)

EDUCATION

- M.Sc., Business Informatics (2014)
  - University of Applied Sciences, Cologne, Germany
- Diploma, Computer Sciences (2007)
  - Frankfurt University of Applied Sciences, Frankfurt, Germany

PROFESSIONAL AFFILIATION

- Chair, UP KRITIS – Critical Infrastructure Protection (CIP) – Working Groups Internet Infrastructure and Audit & Standards
- Chair, ISACA Germany Chapter e.V. – Working Group Information Security (resigned 2018)
- Member, ICANN – Security, Stability, and Resiliency Review (SSR)
- Member, Bitkom – Working Group Security Management
- Member, CENTR – Security and Technical Working Group
- Member, DIN's Standards Committee on IT and Applications (NIA) – Working Groups NA 043-01-27-01 AK and NA 043-01-27-05 AK
- Member, Internet Society German Chapter e.V. (ISOC.DE e.V.)
- Member, OWASP Germany Chapter e.V

DEUTSCHES NETWORK INFORMATION CENTER (DENIC)

Neutral & diskriminierungsfrei	Nicht-gewinnorientierte Genossenschaft	16,7 Mio. .de-Domains	8,3 Mio. Domaininhaber
	Nicht reguliert & unabhängig vom Staat		10 Jahre durchschnittliche Domain-Lebensdauer
285* Genossenschaftsmitglieder 25% im Ausland		Domainverteilung 66 % Unternehmen 31 % Privatpersonen 3 % Organisationen	
Aktive Mitgestaltung des Internets in nationalen & internationalen Gremien	Betrieb Infrastruktur für DNS Anycast Service für ca. 11 Mio. Domains anderer Namensräume		1,5 Mio. Domains mit internationalem Inhaber
18 Eigenbetriebene Nameserver-Standorte weltweit	Betrieb Infrastruktur für Data Escrow Service für Registrare & Registries		ISO/IEC 27001:2013 ISMS ISO 22301:2012 BCMS

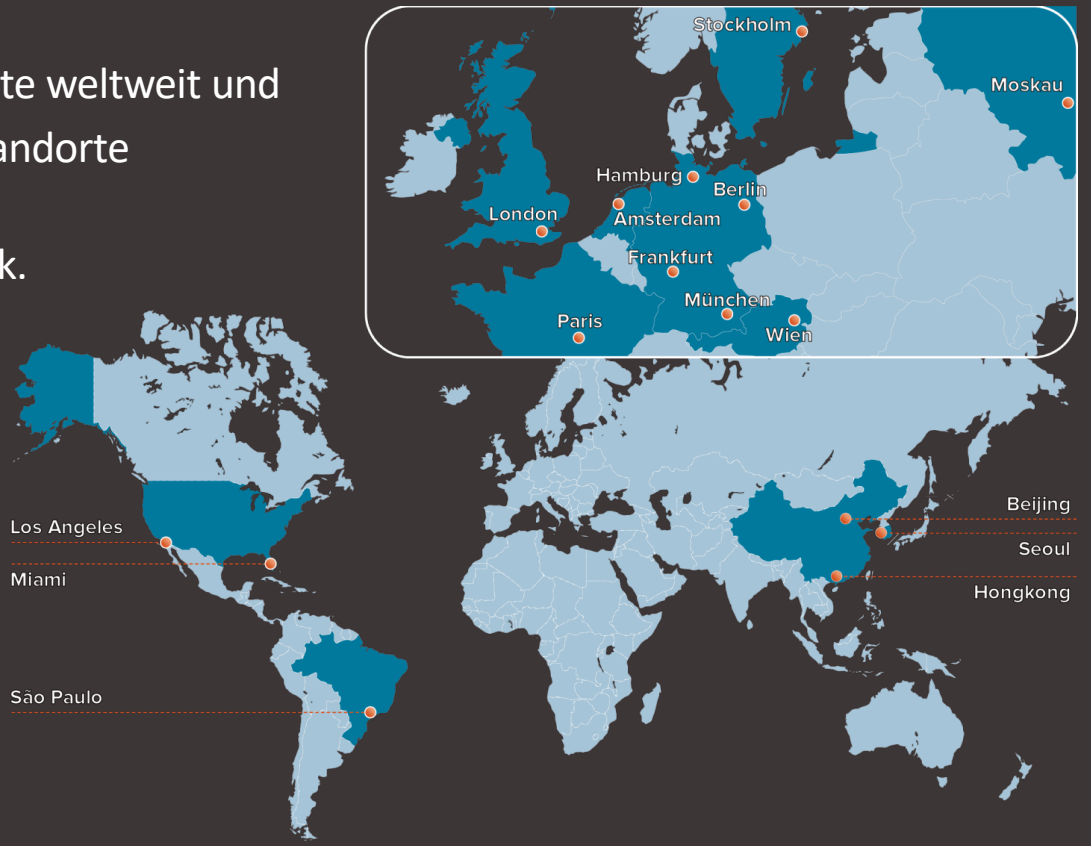
*Stand zum Jahresende unter Berücksichtigung der Austritte, die statuten-gemäß zum 1.1. des Folgejahres wirksam werden

Stand: 31. Dezember 2020

DENIC – NAMESERVICE .DE

- 19 eigene Nameserverstandorte weltweit und
  > 35 ergänzende (Anycast-) Standorte

- > ca. 45.000 DNS-Anfragen/Sek.



UP KRITIS

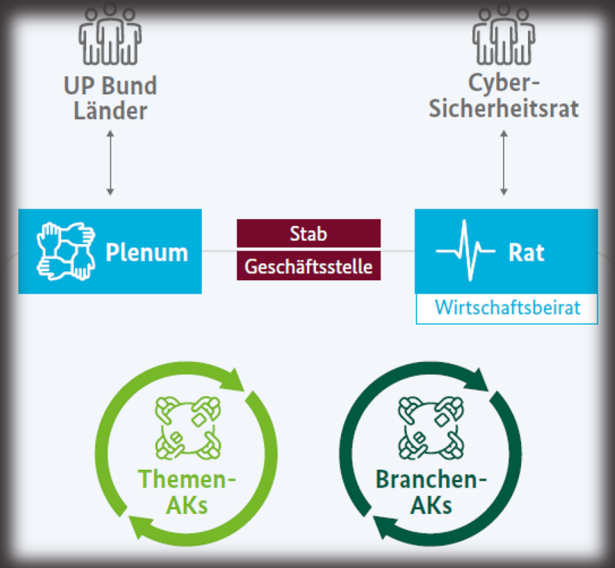
Öffentlich-private Kooperation zwischen

- Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen (BMI, BSI, BBK).
- ca. 740 Teilnehmer

Ziel: Aufrechterhaltung der Versorgung mit kritischen Infrastrukturdienstleistungen in Deutschland

Strategisch-konzeptionelle Zusammenarbeit

- Fachliche und politische Gremien
- Cybersicherheit ist ein Schwerpunkt der Arbeiten
  - Operativer Informationsaustausch



Gremien im UP KRITIS


Let's Get Started

IT-SICHERHEITSGESETZ 1.0 – ÜBERBLICK

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- In Kraft getreten am 25.07.2015
- Identifikation von Betreibern Kritischer Infrastrukturen über BSI-KritisV

Artikelgesetz	Wesentlichen Ziele	Mandat
Das Gesetz umfasst mehrere Änderungen in bestehenden Gesetzen • Gesetz über das Bundesamt für Sicherheit der IT (BSIG) • Telemediengesetz (TMG) • Telekommunikationsgesetz (TKG) • Energiewirtschaftsgesetz (EnWG) • Atomgesetz (AtG)	• Mindestniveau an IT-Sicherheit einzuhalten zum Schutz von Unternehmen und Bürger/Innen, bspw. durch die Umsetzung von branchenspezifischen Sicherheitsstandards (B3S). • Betreiber Kritischer Infrastrukturen müssen dem BSI IT-Sicherheitsvorfälle mit einer hohen Kritikalität melden. • Stärkung des BSI hinsichtlich Rechten, Pflichten und Zuständigkeiten.	• Das BSI kann KRITIS-Betreiber beraten und wird zentrale Meldestelle. • Verpflichtung dem Bundesministerium des Inneren (BMI) jährlich Auskunft zu geben (Lagebild). • Produkte und Systeme auf Sicherheitsaspekte untersuchen. • Erkenntnisse können weitergegeben und veröffentlicht werden.

IT-SICHERHEITSGESETZ – ANFORDERUNGEN AN BETREIBER

- **§ 8a BSIG**
  - Treffen von angemessenen organisatorischen und technischen Vorkehrungen
  - Stand der Technik ist zu berücksichtigen
  - Betreiber können einen Branchenspezifischen Sicherheitsstandard (B3S) vorschlagen
  - Nachweispflicht durch Audits alle 2 Jahre gegenüber dem BSI
- **§ 8b BSIG**
  - BSI als zentrale Meldestelle für Betreiber Kritischer Infrastrukturen
  - Kontinuierliches Lagebild mit Pflicht zur unverzüglichen Weitergabe an Betreiber
  - Alarmierungskontakt ist innerhalb von 6 Monaten zu benennen
  - Verpflichtung zur Meldung von (absehbaren) Sicherheitsvorfällen

WORK in PROGRESS

IT-SICHERHEITSGESETZ 2.0 - WO STEHEN WIR AKTUELL

- 27.03.2019: IT-Sicherheitsgesetz 2.0 (90 Seiten, erster Entwurf)
- 07.05.2020: IT-Sicherheitsgesetz 2.0 (73 Seiten, zweiter Entwurf)
- 19.11.2020: IT-Sicherheitsgesetz 2.0 (92 Seiten, dritter Entwurf)
- 01.12.2020: IT-Sicherheitsgesetz 2.0 (92 Seiten, „Diskussionsentwurf“)
- 09.12.2020: IT-Sicherheitsgesetz 2.0 (108 Seiten, Verbändefassung)
- 11.12.2020: IT-Sicherheitsgesetz 2.0 (119 Seiten)
- 16.12.2020: IT-Sicherheitsgesetz 2.0 (118 Seiten, Kabinettsfassung)
- 01.01.2021: IT-Sicherheitsgesetz 2.0 (130 Seiten, Bundestagsfassung)
- 25.01.2021: IT-Sicherheitsgesetz 2.0 (110 Seiten, Bundestagsfassung)

denic

* Angelehnt an: Cybersecurity-Regulierung 2021: Update, Dr. Dennis-Kenji Kipker, Letzter Aufruf: 24.02.2021

WAS WIRD AKTUELL DISKUTIERT – BEFUGNISAUSBAU BSI

- Tätigkeit als nationale Behörde für die Cybersicherheitszertifizierung
- Entwicklung und Festlegung des Stands der Technik durch das BSI
- Ausbau der Funktion des BSI als allgemeine Meldestelle
- Krisenreaktion: Federführende Entwicklung “Gesamtplanes für Reaktionsmaßnahmen des Bundes”
- Detektion von Sicherheitslücken in öffentlich erreichbaren Systemen
- Erhebliche Störungen: Anforderungsrecht für bestimmte (auch personenbezogene) Daten und Eingriffsbefugnis in Systeme und unternehmerische Prozesse zu ihrer Wiederherstellung

WAS WIRD AKTUELL DISKUTIERT – BETREIBERPFLICHTEN

- Implementierung eines Systems zur Angriffserkennung mit dem Ziel der Störungsvermeidung, Informationsweitergabe an das BSI
- Übermittlung einer Liste aller IT-Produkte mit Bedeutung für die Funktionsfähigkeit der Kritischen Infrastruktur an das BSI
- Erweiterung: Unternehmen im besonderen öffentlichen Interesse (mehrfache Änderung der Bezugspunkte und Bestimmungsgrößen, unklare Anknüpfungspunkte) mit ggü. KRITIS herabgesetzten Pflichten

WAS WIRD AKTUELL DISKUTIERT – HERSTELLER

- Freiwilliges nationales IT-Sicherheitskennzeichen
- Einsatz von kritischen Komponenten und Garantieerklärung des Herstellers
- Meldepflichten im Kontext von Schwachstellen beim Einsatz in KRITIS-Komponenten

STELLUNGNAHMEN UND KRITIK

- Gesetzgebungsverfahren und Rechtssicherheit
  - Beteiligung, Fristen als auch essentielle Festlegungen durch BSI-KritisV
- Bestimmung der Unternehmen im besonderen öffentlichen Interesse
  - Kriterien und Rechtssicherheit, Notwendigkeit
- Verarbeitung von Protokolldaten und Bestandsdatenauskunft
  - Umfassende Speichermöglichkeiten für Protokoll- und Bestandsdaten
- Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit
  - Fehlende Vorankündigung von Maßnahmen
- Unübersichtliche Bußgeldvorschriften
  - Vereinheitlichung EU DS-GVO, dann wieder Verweise auf OWiG

WAS IST GEBLIEBEN? – STAND JETZT!

- Ergänzung Siedlungsabfallentsorgung als KRITIS im BSIG
- Regelung und Definition von „Kritischen Komponenten“ sowie von „Unternehmen im besonderen öffentlichen Interesse“
- Aufgabenfestlegungen BSI: Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte
- Umfassende Kontrollmöglichkeiten der Kommunikationstechnik des Bundes seitens BSI
- BSI als allgemeine Meldestelle für Sicherheit in der IT, weiterer Ausbau und Datenumgang

WAS IST GEBLIEBEN? – STAND JETZT!

- Erhebung und Verarbeitung von Protokollierungsdaten, die durch den Betrieb der Kommunikationstechnik des Bundes anfallen
- Bestandsdatenauskunft des BSI bei TK-Anbietern, auch nach IP-Adressen inkl. Übermittlungsbefugnis personenbezogener Daten
- Untersuchungsmöglichkeit der Sicherheit in der Informationstechnik inkl. Weiterübermittlungsbefugnisse an weitere Behörden
- Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden (Portscans) anhand „weißer Liste“.
- Anordnungsbefugnisse zur IT-Sicherheit ggü. TK-Diensteanbietern

WAS IST GEBLIEBEN? – STAND JETZT!

- Anordnung der Verwendung von Systemen zur Angriffserkennung durch KRITIS-Betreiber
- Datenherausgabepflicht von KRITIS-Betreibern ggü. BSI zur Bewältigung erheblicher Störungen
- TOM-Regelungen zur IT-Sicherheit von Unternehmen im besonderen öffentlichen Interesse ggü. Betreibern abgeschwächt (u.a. Selbsterklärung), Registrierung und Kontaktstelle, Meldepflichten
- Untersagung des Einsatzes kritischer Komponenten: Anzeigepflicht vor Einsatz in KRITIS, Garantieerklärung des Herstellers, Untersagungsbefugnis des BMI

WAS IST GEBLIEBEN? – STAND JETZT!

- Freiwilliges IT-Sicherheitskennzeichen: Festlegung durch TR des BSI und konkretisierende Rechtsverordnung, Freigabe durch BSI vor Verwendung
- Bußgeldvorschriften: Abstufungen 2 Millionen Euro, 1 Million Euro, 500.000 Euro, 100.000 Euro, vgl. auch bisherige Kritik

ZEITPLAN

- Beschlussfassung Bundeskabinett am 16.12.2020
- Zurzeit Notifizierung durch EU-Kommission (Dauer ca. drei Monate)
- Erste Lesung im Bundestag 28.01.2021, weitere Anhörung 01.03.2021
- Möglicher Termin zur Verabschiedung: Letzte Sitzungswoche vor Ostern (22.03.2021 - 26.03.2021)
- Wahrscheinlich: Verabschiedung vor der parlamentarischen Sommerpause (Ende der Legislaturperiode)

DANKE !

FRAGEN ?

KONTAKT:

boban@denic.de