DIE NIS-RICHTLINIE UND DER RECHTLICHE RAHMEN VON CERTS

VORTRAG IM RAHMEN DER IT FRAUD TAGUNG 2017
AM 16. MÄRZ 2017 IN SALZBURG

Ing. Dr. iur. Christof Tschohl

wissenschaftlicher Leiter

Research Institute AG & Co KG

Zentrum für Digitale Menschenrechte

Das Projekt CERT-Kommunikationsmodell II (CERT-Komm II)

- CERT: Computer emergency response team
- CSIRT: Computer security incident response teams

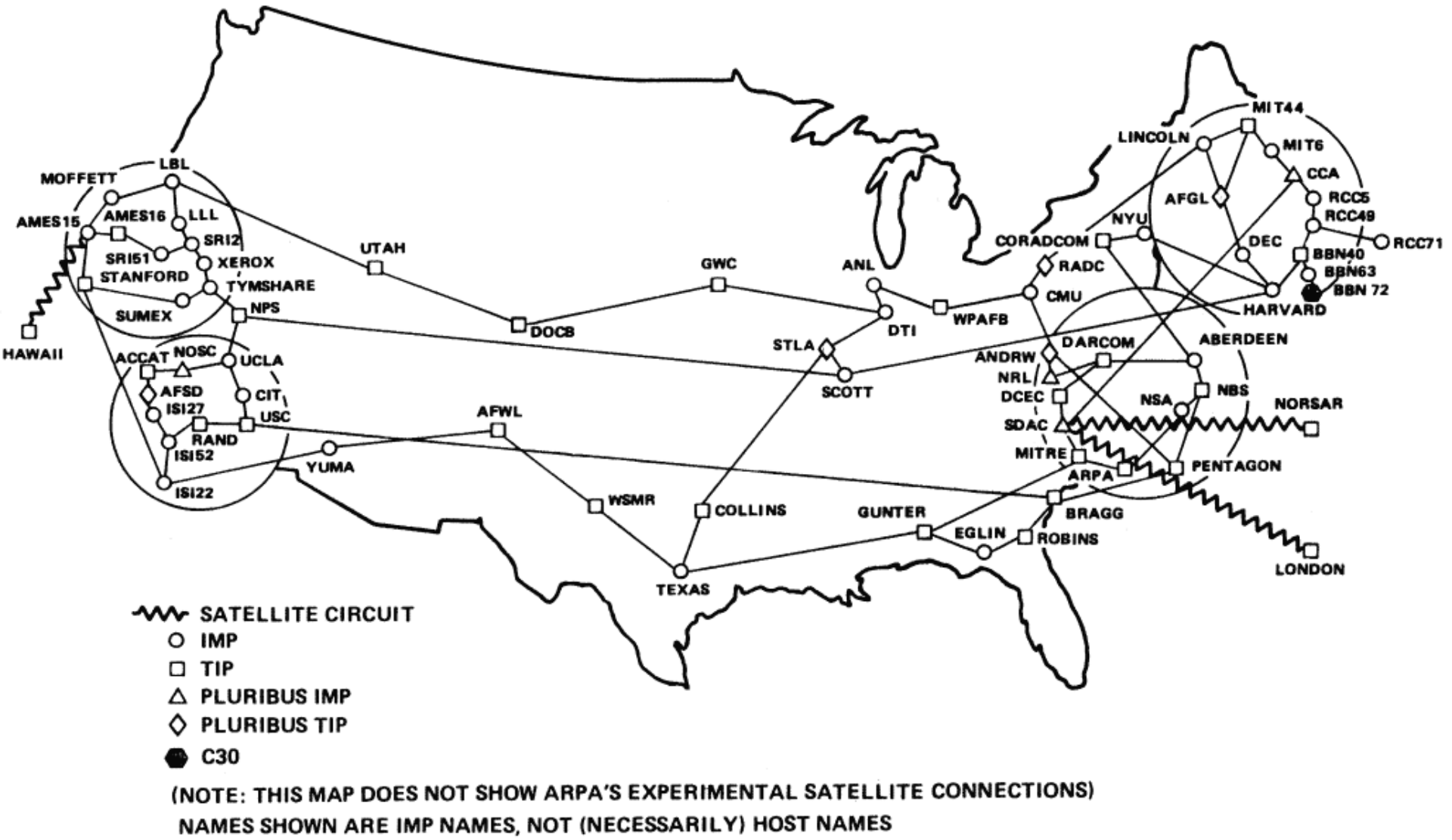
- Projektziel: CERT-Kommunikation unterstützen:
  - Compliance absichern
  - Vertrauen erhöhen

- Die Projekte CERT-Komm und CERT-Komm II wurden bzw. werden finanziert im Sicherheitsforschungs-Förderprogramm KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie..

Agenda

- CERTs und ihre Entwicklung
- CERT-Rahmenbedingungen
- NIS-Richtlinie und CERTs/CSIRTs
- Regelungsbedarf im Cybersicherheitsgesetz
- Ausblick

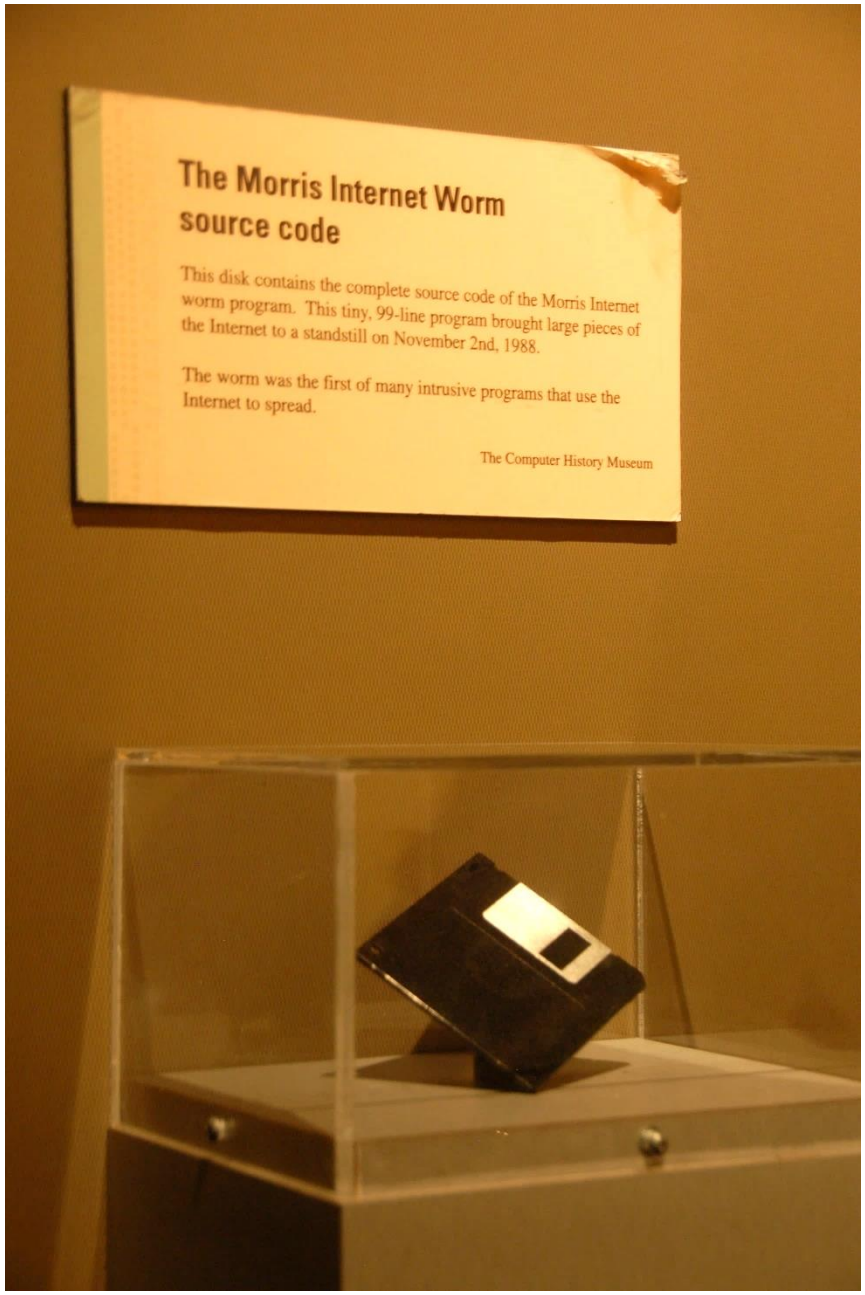
ARPANET GEOGRAPHIC MAP, OCTOBER 1980



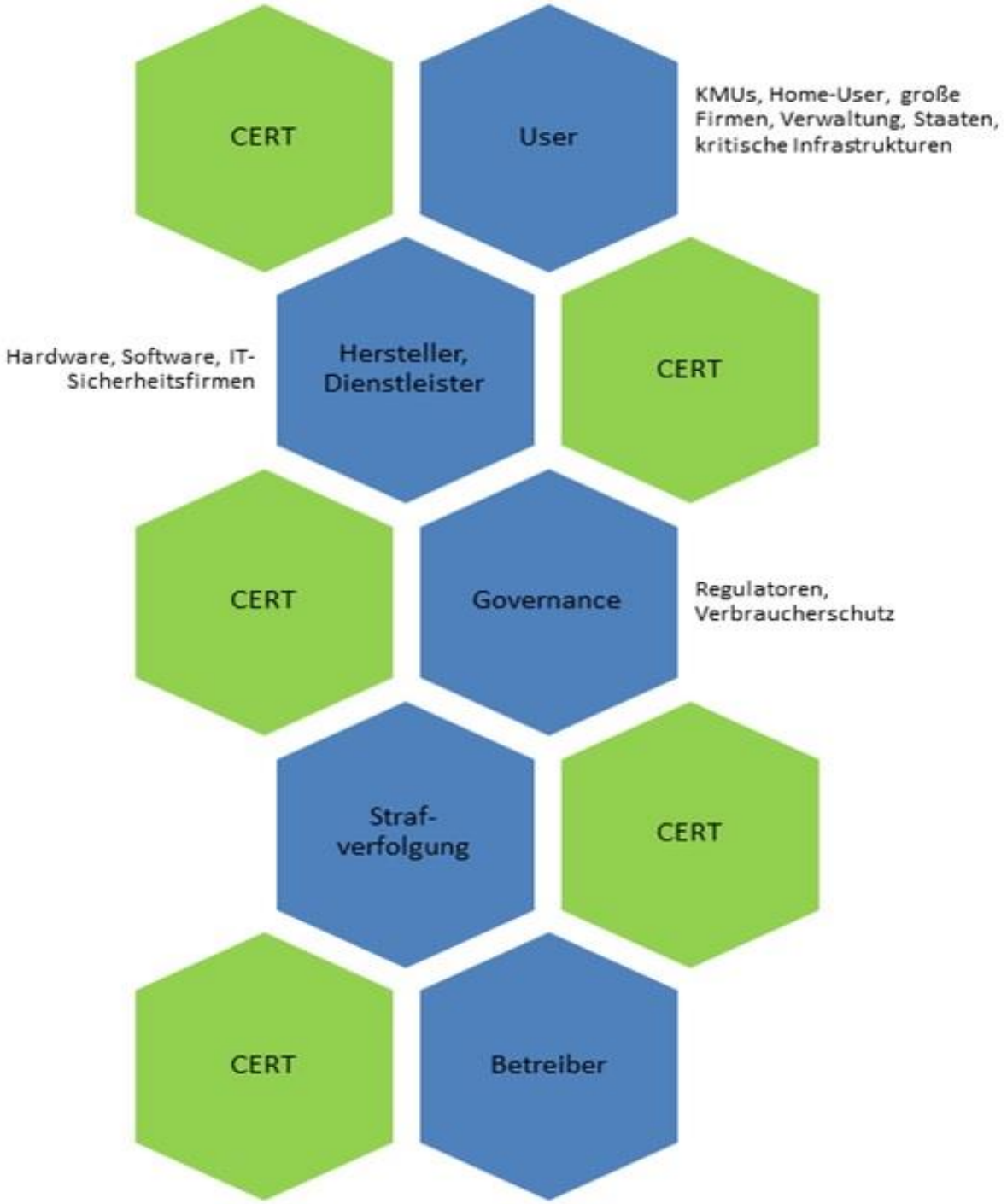
(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html, 21.2.17

Morris Wurm, 1988



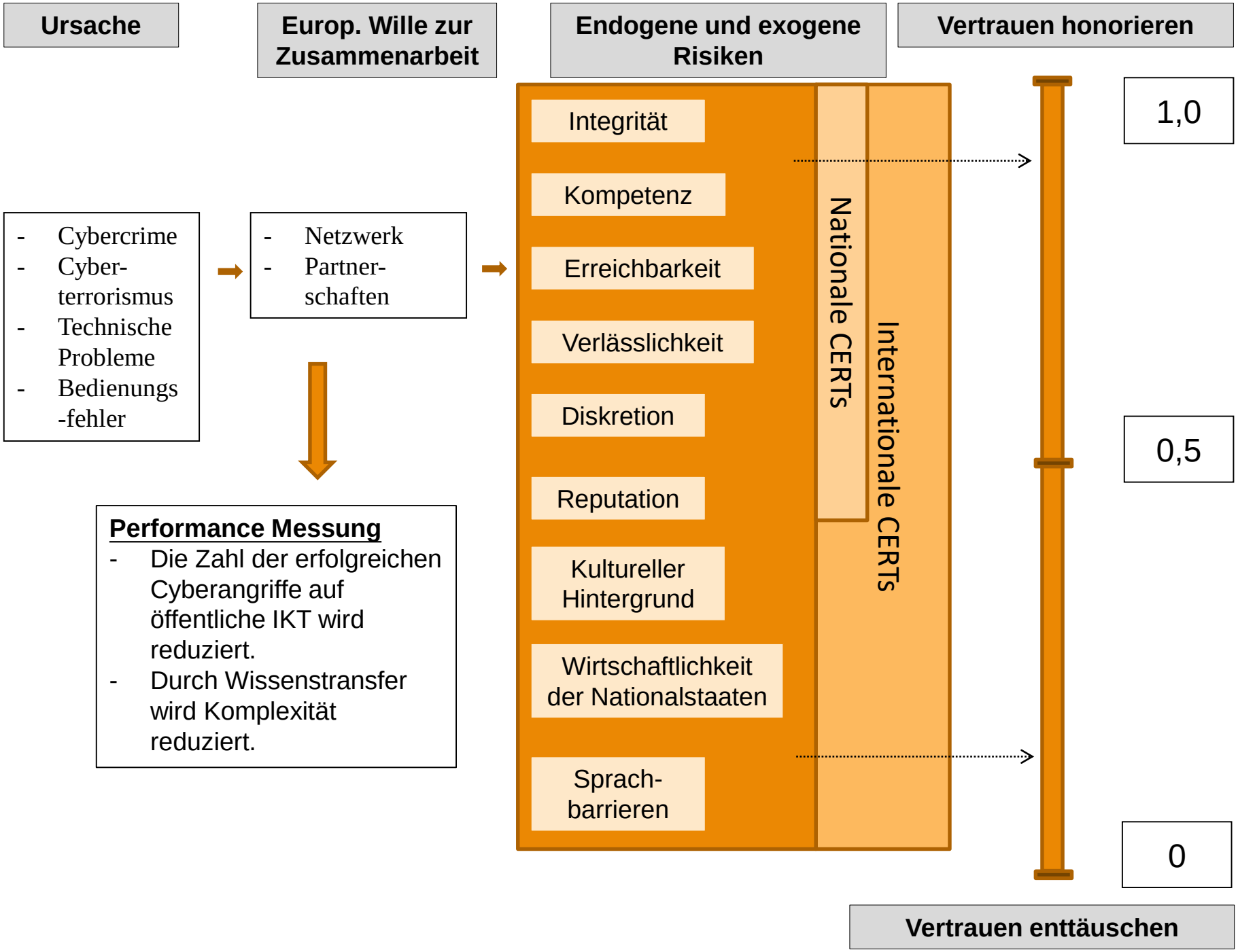
http://thisdayintechhistory.com/11/02/morris-worm-tunnels-through-internet/, 21.2.17


CERT
User
KMUs, Home-User, große Firmen, Verwaltung, Staaten, kritische Infrastrukturen
Hardware, Software, IT-Sicherheitsfirmen
Hersteller, Dienstleister
CERT
CERT
Governance
Regulatoren, Verbraucherschutz
Straf-verfolgung
CERT
CERT
Betreiber

CERT HANDLUNGSMÖGLICHKEITEN

- Nationales CERT: Koordination, Empfehlungen, Publikationen, Pressearbeit
- Firmen CERT: konkrete Anweisung bis Sperre Internet-Anschluss
- Produkt CERT: Empfehlungen
- GovCERT: Koordination, Empfehlungen
- CERT im Bereich Kritische Infrastruktur: siehe Beispiel

- Und auf welcher rechtlichen Basis?
- Und wie erfahren sie von den IT-Sicherheitszwischenfällen, die für sie relevant sind?


Ursache
Europ. Wille zur Zusammenarbeit
Endogene und exogene Risiken
Vertrauen honorieren
- Cybercrime
- Cyber-terrorismus
- Technische Probleme
- Bedienungs-fehler
- Netzwerk
- Partner-schaften
Performance Messung
- Die Zahl der erfolgreichen Cyberangriffe auf öffentliche IKT wird reduziert.
- Durch Wissenstransfer wird Komplexität reduziert.
Integrität
Kompetenz
Erreichbarkeit
Verlässlichkeit
Diskretion
Reputation
Kultureller Hintergrund
Wirtschaftlichkeit der Nationalstaaten
Sprach-barrieren
Nationale CERTs
Internationale CERTs
1,0
0,5
0
Vertrauen enttäuschen

Aktuelles CERT-Umfeld

- Incidents, Cyber-Sicherheitsvorfälle: mannigfaltig
- Schwachstellen: zahllos
- Bedrohungen durch:
  - Cyber-Kriminelle, Terroristen
  - Technische Probleme
  - Staatliche Akteure, Spionage
- Akteure im Internet:
  - Mit unterschiedlichen Interessen

- Siehe:
  - IOCTA Bericht Europol
  - ENISA Threat Landscape Report 2016

Agenda

- CERTs und ihre Entwicklung
- CERT-Rahmenbedingungen
- NIS-Richtlinie und CERTs/CSIRTs
- Regelungsbedarf im Cybersicherheitsgesetz
- Ausblick

Richtlinie zur Netz- und Informationssicherheit (NIS-RL)

- Am 6. Juli 2016 verabschiedet → EU-Richtlinie zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-Richtlinie).
- Die Mitgliedstaaten müssen eine **Netzwerk- und Informationssicherheitsstrategie** festlegen (Art 7)
- Die Mitgliedstaaten müssen eine **Liste von Betreibern wesentlicher Dienste** erstellen (Art 5)
- Die Mitgliedstaaten müssen **zuständige Behörden**, **nationale Anlaufstellen** und **CSIRTs** benennen (Art 8)
- **Kooperationsgruppe** für strategische Zusammenarbeit und Informationsaustausch zwischen den Mitgliedstaaten (Art 11)
- **Netzwerk der nationalen CSIRTs** (Art 12)
- **Sicherheitsanforderungen** und **Meldepflichten** für Betreiber wesentlicher Dienste (Art 14) und Anbieter digitaler Dienste (Art 16)
- **Freiwillige Meldung** (Art 20) durch andere Einrichtungen

BEHÖRDEN

- Art 8 Abs 1: Benennung einer oder mehrerer für die Netz- und Informationssicherheit **zuständiger Behörden (NIS-Behörden)**, entweder bestehende oder neue Behörde(n)
- Art 8 Abs 3 f: „**Zentrale Anlaufstelle**“ (SPOC) als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit der Behörden
- Art 9: Computer Security Incident Response Teams (CSIRTs)
- Es kann sich um 1, 2, 3 oder mehrere Behörden handeln
- Art 10 Abs 2: Die Mitgliedstaaten stellen sicher, dass **entweder die NIS-Behörden oder die CSIRTs** die gemäß dieser Richtlinie übermittelten Meldungen von Sicherheitsvorfällen erhalten.
- Art 15 Abs 1, Art 17 Abs 1: **NIS-Behörden überprüfen die Einhaltung der Pflichten** durch Betreiber wesentlicher Dienste und Anbieter digitaler Dienste (hier nur eingeschränkt, ex-post)

CSIRTs

Art 9 Abs 1: Jeder Mitgliedstaat hat **eines oder mehrere CSIRTs zu benennen**, die für die Bewältigung von Risiken und Vorfällen **nach einem genau festgelegten Ablauf** zuständig sind und **mindestens folgende Sektoren und Dienste abdecken**:

Sektoren:

- Energie
  - Elektrizität
  - Erdöl
  - Erdgas
- Verkehr
  - Luftverkehr
  - Schienenverkehr
  - Schifffahrt
  - Straßenverkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen (Einrichtungen der medizinischen Versorgung)
- Trinkwasserlieferung und -versorgung
- Digitale Infrastruktur

Dienste:

- Online-Marktplätze
- Online-Suchmaschinen
- Cloud-Computing-Dienste

Anforderungen an CSIRTs (Anhang I Abs 1 NIS-RL)

a) CSIRTs sorgen für einen hohen Grad der **Verfügbarkeit ihrer Kommunikationsdienste**, indem sie punktuellen Ausfällen vorbeugen und mehrere Kanäle bereitstellen, damit sie jederzeit erreichbar bleiben und selbst Kontakt aufnehmen können. Die Kommunikationskanäle müssen zudem genau spezifiziert und den CSIRT-Nutzern ("Constituency") und den Kooperationspartnern wohlbekannt sein.

b) Die Räumlichkeiten der CSIRTs und die unterstützenden Informationssysteme werden an **sicheren Standorten** eingerichtet.

c) **Betriebskontinuität**:

   i. CSIRTs müssen über ein geeignetes **System** zur Verwaltung und Weiterleitung von Anfragen verfügen, um Übergaben zu erleichtern.

   ii. CSIRTs müssen personell so ausgestattet sein, dass sie eine **ständige Bereitschaft** gewährleisten können.

   iii. CSIRTs müssen auf eine **Infrastruktur** gestützt sein, deren **Verfügbarkeit** sichergestellt ist. Zu diesem Zweck müssen **Redundanzsysteme** und **Ausweicharbeitsräume** zur Verfügung stehen.

d) CSIRTs müssen die Möglichkeit haben, sich an internationalen Kooperationsnetzen zu beteiligen, wenn sie es wünschen.

AUFGABEN DER CSIRTS (ANHANG I ABS 2 NIS-RL)

a) Die Aufgaben der CSIRTs umfassen mindestens Folgendes:
   i. **Überwachung von Sicherheitsvorfällen** auf nationaler Ebene.
   ii. Ausgabe von **Frühwarnungen** und **Alarmmeldungen** sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interessenträgern.
   iii. **Reaktion** auf Sicherheitsvorfälle.
   iv. dynamische **Analyse** von Risiken und Vorfällen und Lagebeurteilung.
   v. Beteiligung am CSIRTs-Netzwerk.

b) CSIRTs bauen Kooperationsbeziehungen zum Privatsektor auf.

c) Zur Erleichterung der Zusammenarbeit fördern CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für:
   i. Abläufe zur Bewältigung von Sicherheitsvorfällen und Risiken;
   ii. Systeme zur Klassifizierung von Sicherheitsvorfällen, Risiken und Informationen.

Die Mitgliedstaaten haben die CSIRTs mit angemessenen **Ressourcen** zur Erfüllung dieser Aufgaben auszustatten (Art 9 Abs 2) und sicherzustellen, dass sie „Zugang zu einer angemessenen, sicheren und robusten Kommunikations- und Informationsinfrastruktur auf nationaler Ebene haben“ (Art 9 Abs 3).

CSIRT-KOOPERATION/ CSIRTS-NETZWERK

- Art 10 Abs 1: Nationale Zusammenarbeit mit der NIS-Behörde zur Erfüllung der in der NIS-RL festgelegten Pflichten
- Art 12: Europäisches CSIRTs-Netzwerk (aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU) für primär operative Aufgaben:
  - a) Informationsaustausch zu den Diensten, Tätigkeiten und Kooperationsfähigkeiten der CSIRTs
  - b) auf Antrag des Vertreters eines CSIRT eines von einem Sicherheitsvorfall potenziell betroffenen Mitgliedstaats Austausch und Erörterung von wirtschaftlich nicht sensiblen Informationen im Zusammenhang mit diesem Vorfall und damit verbundenen Risiken; das CSIRT eines jeden Mitgliedstaats kann jedoch die Beteiligung an diesen Erörterungen ablehnen, wenn die Gefahr einer Beeinträchtigung der Untersuchung des Vorfalls besteht
  - c) Austausch und Bereitstellung auf freiwilliger Basis von nicht vertraulichen Informationen zu einzelnen Sicherheitsvorfällen
  - d) auf Antrag des Vertreters des CSIRT eines Mitgliedstaats Erörterung und – sofern möglich – Ausarbeitung einer koordinierten Reaktion auf einen Sicherheitsvorfall, der im Gebiet dieses Mitgliedstaats festgestellt wurde
  - e) Unterstützung der Mitgliedstaaten bei der Bewältigung grenzüberschreitender Sicherheitsvorfälle auf der Grundlage einer freiwilligen gegenseitigen Unterstützung

CSIRT-KOOPERATION

f) Erörterung, Sondierung und Bestimmung weiterer Formen der operativen Zusammenarbeit, unter anderem im Zusammenhang mit
   i. Kategorien von Risiken und Sicherheitsvorfällen,
   ii. Frühwarnungen,
   iii. gegenseitiger Unterstützung,
   iv. Grundsätzen und Modalitäten der Koordinierung bei der Reaktion der Mitgliedstaaten auf grenzüberschreitende Risiken und Vorfälle

g) Unterrichtung der Kooperationsgruppe über seine Tätigkeiten und über die gemäß Buchstabe f erörterten weiteren Formen der operativen Zusammenarbeit, und Ersuchen um Leitlinien dafür

h) Erörterung der aus den Übungen zur Sicherheit von Netz- und Informationssystemen, auch den von der ENISA organisierten derartigen Übungen – gezogenen Lehren

i) auf Antrag eines einzelnen CSIRT Erörterung der Fähigkeiten und der Abwehrbereitschaft dieses CSIRT

j) Erstellung von Leitlinien zur Erleichterung der Konvergenz der operativen Verfahrensweisen in Bezug auf die Anwendung der Bestimmungen dieses Artikels betreffend die operative Zusammenarbeit

ErwGr 40: Sekretariat des CSIRTs-Netzwerks unterhält eine **Website** „auf der allgemeine **Informationen über größere in der Union aufgetretene Sicherheitsvorfälle** mit einem besonderen Schwerpunkt auf die Interessen und den Bedarf von Unternehmen der allgemeinen Öffentlichkeit zur Verfügung gestellt werden. CSIRTs, die sich am CSIRTs-Netzwerk beteiligen, werden aufgefordert, **freiwillig** die auf dieser Website zu veröffentlichenden **Informationen bereitzustellen**, ohne vertrauliche oder sensible Informationen darin aufzunehmen.“

Meldepflicht der Betreiber wesentlicher Dienste (ggf. an CSIRTs)

- **Betreiber wesentlicher Dienste** müssen Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben, der zuständigen Behörde oder dem CSIRT unverzüglich melden (Art 14 Abs 3 NIS-RL).
- Ebenso müssen **Anbieter digitaler Dienste** Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Union erbrachten digitalen Dienstes haben (Art 16 Abs 3 NIS-RL).
  - Erheblichkeitskriterien: Art 14 Abs 4 und Art 16 Abs 4
  - Umstände, die eine solche Meldepflicht auslösen, können in nationalen Leitlinien (Art 14 Abs 7) bzw. in Durchführungsrechtsakten (Art 16 Abs 8) näher geregelt werden.
- Die zuständige Behörde oder das CSIRT **unterrichten andere Mitgliedstaaten von Vorfällen**, wenn diese erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in diesen Mitgliedstaaten hat, wobei die Sicherheit und das wirtschaftliche Interesse des Betreibers wesentlicher Dienste sowie die Vertraulichkeit der in dessen Meldung bereitgestellten Informationen zu wahren sind (Art 14 Abs 5, Art 16 Abs 6).
- Die zuständige Behörde oder das CSIRT können nach Anhörung des meldenden Betreibers **die Öffentlichkeit über einzelne Sicherheitsvorfälle** unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist (Art 14 Abs 6, Art 16 Abs 7).

Freiwillige Meldungen

- Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden und die keine Anbieter digitaler Dienste sind, können freiwillig Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen angebotenen Dienste haben (Art 20 Abs 1). Solche Meldungen sind nach dem in Art 14 für verpflichtende Meldungen festgelegten Verfahren zu behandeln.
- Ebenso können Betreiber wesentlicher Dienste und Anbieter digitaler Dienste freiwillig Sicherheitsvorfälle melden, die keine Meldepflicht auslösen, weil sie die Erheblichkeitsschwelle nicht überschreiten.
- Kernfrage: Wie können Einrichtungen zu freiwilligen Meldungen motiviert werden?
  - Eine freiwillige Meldung darf nicht dazu führen, dass der meldenden Einrichtung Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie den Vorfall nicht gemeldet hätte (Art 20 Abs 2).
  - Eine freiwillige Meldung kann jedoch eine Verpflichtung offenlegen.
  - Ein freiwillige Meldung kann zu unerwünschter Aufmerksamkeit führen, insbesondere, wenn sie unmittelbar ein Strafverfahren nach sich zieht.
  - Meldung an (Branchen-)CERT (gesetzlich beliehen; keine Anzeigepflicht)

Cybersicherheitsgesetz: Anforderungen

- Österreichische Umsetzung der NIS-Richtlinie
- Rechtliche Grundlage für CERTs, insbesondere für Datenverarbeitung und Datenaustausch
  - zum Teil (datenschutz-)rechtlich erforderlich
  - jedenfalls aber sinnvoll, denn Rechtssicherheit trägt zum (raschen) Funktionieren des Systems bei
  - Sicherstellung, dass sich Befugnisse und Aktivitäten von CERTs innerhalb grundrechtlicher Schranken bewegen
  - Normierung einer strengen Akzessorietät zwischen Aufgaben und Befugnissen
- Gesetz soll Klarheit schaffen, was von den CERTs erwartet wird
  - Rechtsnatur der verschiedenen CERTs
  - Rolle von CERT.at zwischen GovCERT und Unternehmens-CERTS

AUSBLICK

- Nationale Gestaltung NIS-RL
- CERTs bei Informationsaustausch unterstützen
- Ausgewogenheit zwischen
  - polizeilichen und militärischen

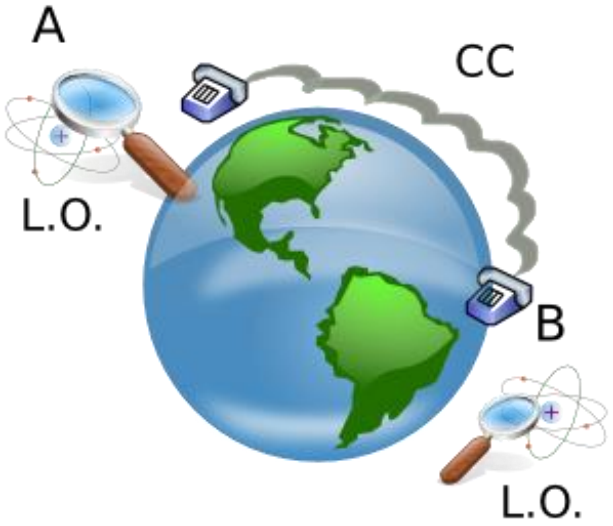
  sowie
  - zivilen bzw. wirtschaftliche Dimensionen

  sicherstellen

Nationale Sicherheit vs. Vertrauen Kooperation

VIELEN DANK

FÜR IHRE AUFMERKSAMKEIT!



TITEL DES VORTRAGS:
DIE NIS-RICHTLINIE UND DER RECHTLICHE RAHMEN VON CERTS

Forschungserkenntnisse und Ausarbeitung der Präsentation im Rahmen des KIRAS Projekts CERT Komm II durch

Christof Tschohl / Walter Hötzendorfer / Gerald Quirchmayr / Edith Huber / Otto Hellwig

KIRAS Sicherheitsforschung | BUNDESKANZLERAMT ÖSTERREICH | SBA Research | universität wien | DONAU UNIVERSITÄT KREMS | research institute | IKARUS security software

(Definitionen)

Art 14 Abs 17-19 NIS-RL: Für die Zwecke der NIS-RL bezeichnet der Ausdruck:

- "Online-Marktplatz" einen digitalen Dienst, der es Verbrauchern und/oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a bzw. Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates**1** ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern entweder auf der Website des OnlineMarktplatzes oder auf der Website eines Unternehmers, die von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, abzuschließen;
- "Online-Suchmaschine" einen digitalen Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, und der daraufhin Links anzeigt, über die Informationen im Zusammenhang mit dem angeforderten Inhalt gefunden werden können;
- "Cloud-Computing-Dienst" einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht;

RESEARCH INSTITUTE AG & CO KG
ZENTRUM FÜR DIGITALE MENSCHENRECHTE

Das **Research Institute (RI)** ist ein junges Forschungszentrum an der Schnittstelle von **Technik, Recht** und **Gesellschaft**, das sich aus multi- und interdisziplinärer Perspektive mit der Bedeutung der Menschenrechte im digitalen Zeitalter beschäftigt.

Portfolio:

- **Forschung zu technischen** und **rechtlichen** Aspekten von **Datenschutz** und **Datensicherheit, Cybercrime, Technikfolgenabschätzung** und **Netzpolitik**
- **smart.rights.consulting:** Beratung in datenschutzrechtlichen Fragen
- **Schulungen** für Privatpersonen und Mitarbeiter von Unternehmen/Organisationen
- **Maßgeschneiderte technische Lösungen** zur praktischen Umsetzung der Compliance-Prozesse (in Zusammenarbeit mit Software-Entwicklern)
- **Konzeption und Durchführung individueller und multidisziplinärer Projekte** mit den besten Partnern auf nationaler und internationaler Ebene.

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte
smart.rights.consulting

TEAM

Ing. Dr. iur. Christof Tschohl
Wissenschaftlicher Leiter | Gesellschafter | Prokurist
christof.tschohl@researchinstitute.at

Georg Benedikt Schmidt
Geschäftsführer| Gesellschafter | Softwareentwickler

DI Dr. iur. Walter Hötzendorfer
Senior Researcher | Senior Consultant
walter.hoetzendorfer@researchinstitute.at

Web: http://www.researchinstitute.at