"T.I.S.P. Community Meeting 2020"

Berlin, 03.-04.11.2020

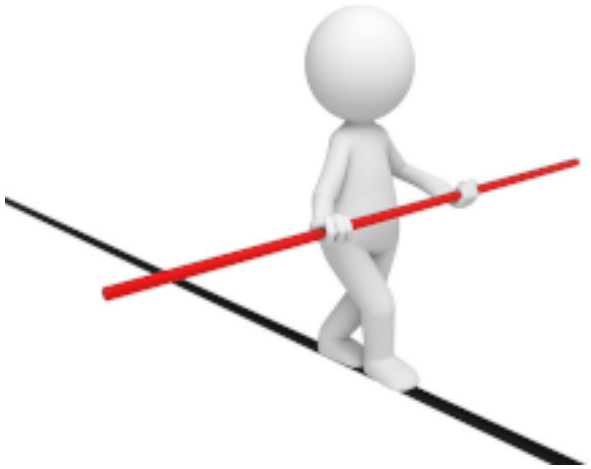
CERTs – Entwicklungen, Strukturen, Status

Prof. Dr. Klaus-Peter Kossakowski / HAW Hamburg

CERTs

Entwicklung, Strukturen, Status

Prof. Dr. Klaus-Peter Kossakowski



Was waren 1973 im Internet die drei schwerwiegensten Sicherheitsprobleme?

RFC 602:

1. Passwörter
2. Schwachstellen
3. „kreative“ Nutzer*innen

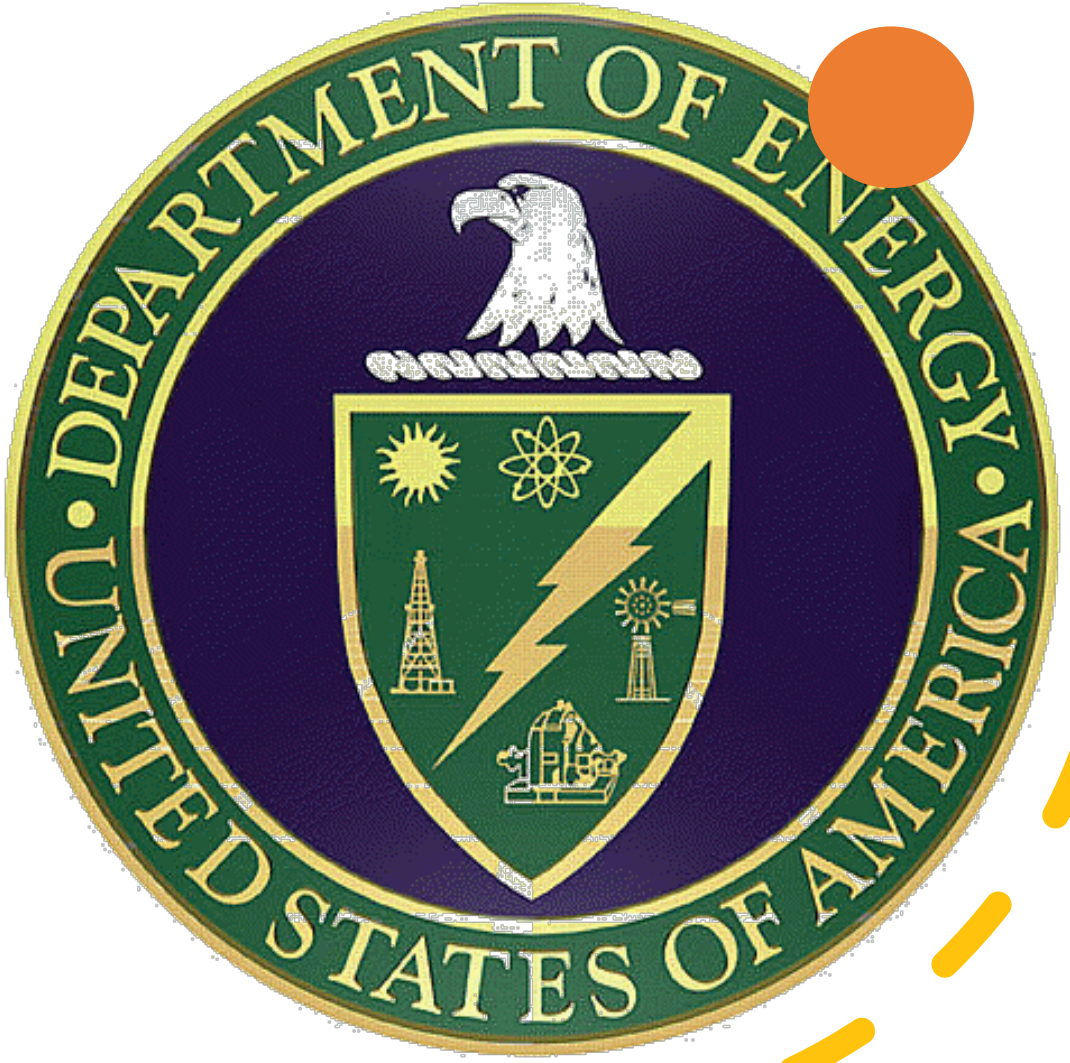
2. November 1988

- **2. November 1988: Internet-Wurm**
  - Internet besteht aus ca. 70.000 Rechner
  - Etwas weniger als 10% befallen
  - Kommunikationsinfrastruktur effektiv ausgeschaltet
- **6. Dezember 1988: DARPA-Krisensitzung**
  - Analyse der Angriffe: Okay
  - Korrektur der Ursachen: Okay
  - Behebung der Schäden: Teilweise
  - Kommunikation / Koordination: NULL

Aber warum gab es damals nichts!?!

Tatsächlich war man aufgrund der vielen – erfolgreichen – Angriffe bereits 1987 auf die Idee gekommen, CERT-Prozesse als Erweiterung des Risikomanagements aufzubauen …

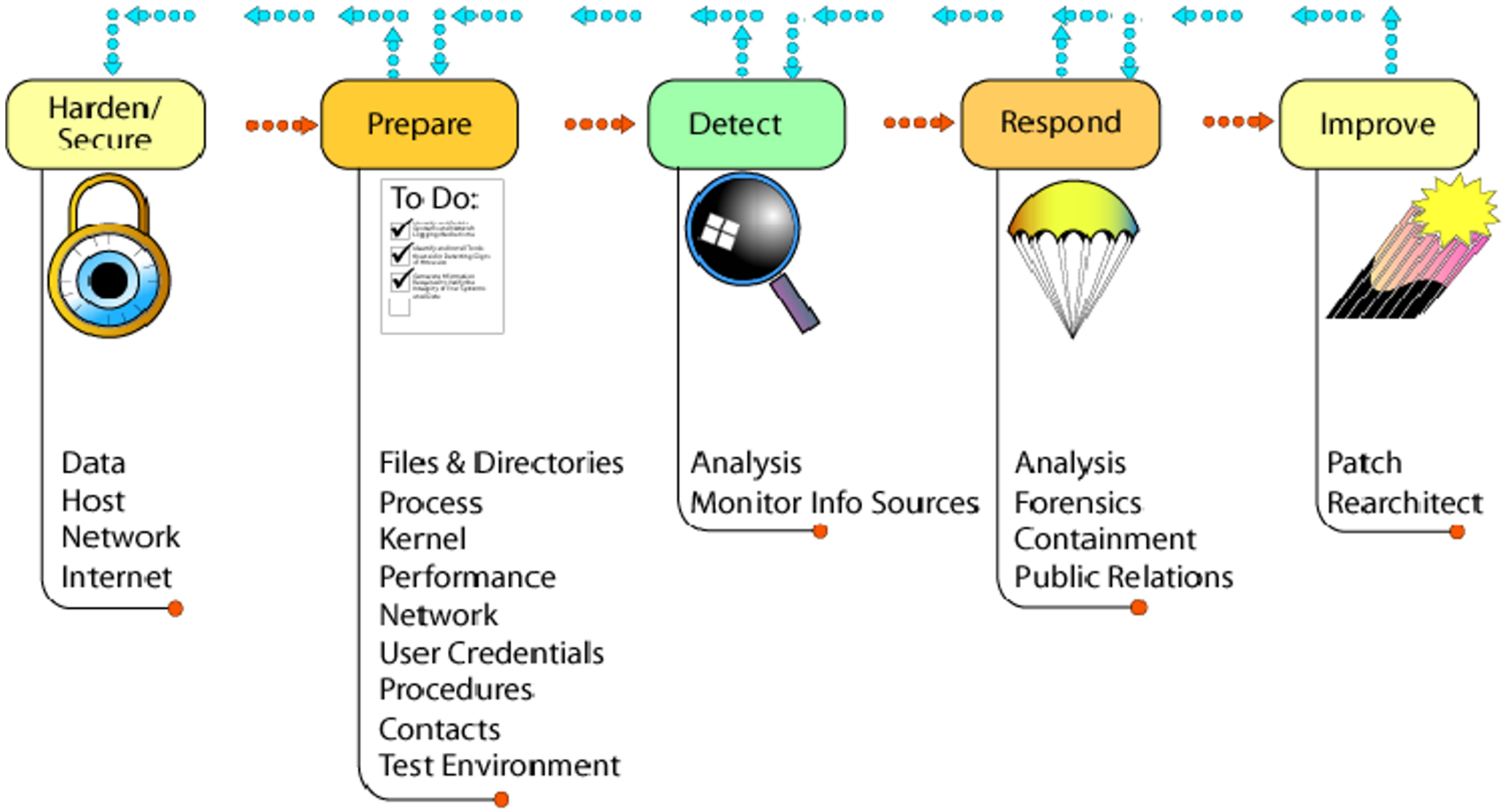
- Rick Carr, US DoE



Erstes CERT in Deutschland

- **1991 : Zu viele Vorfälle in Europa**
  - Europäische Forschungsnetze starten den Informationsaustausch
- **1992 : Ausschreibung des DFN**
  - ca. 70.000 Rechner in Deutschland
- **1993 : Das Internet hebt ab**
  - der Kollege nebenan programmiert einen Web-Server selbst
  - erste Vorfälle machen weitere Diskussion unnötig

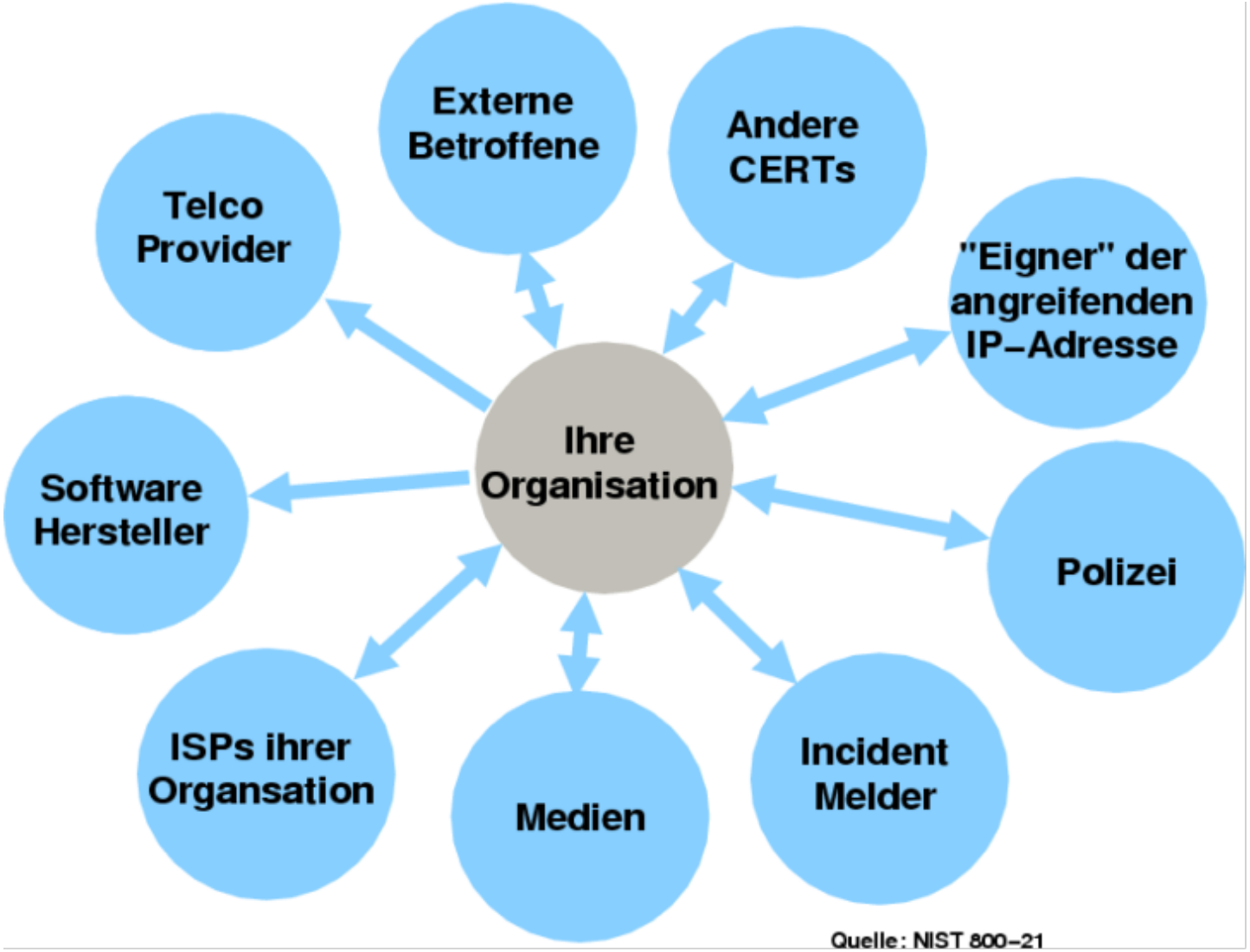
Worum geht es bei CERTs? Response!



Copyright 2001 Carnegie Mellon University

Incident Management ist ein Process!

Den Kontakt nach draußen braucht es!



Merke:

Nach dem Vorfall ist vor dem Vorfall!

Schritte zur ganzheitlichen Sicherheit

Alle Risiken bewerten und „im Blick“ halten

Initiale Bewertung, dann kontinuierlich Lagebild und Sicherheits- bzw. Warnmeldungen

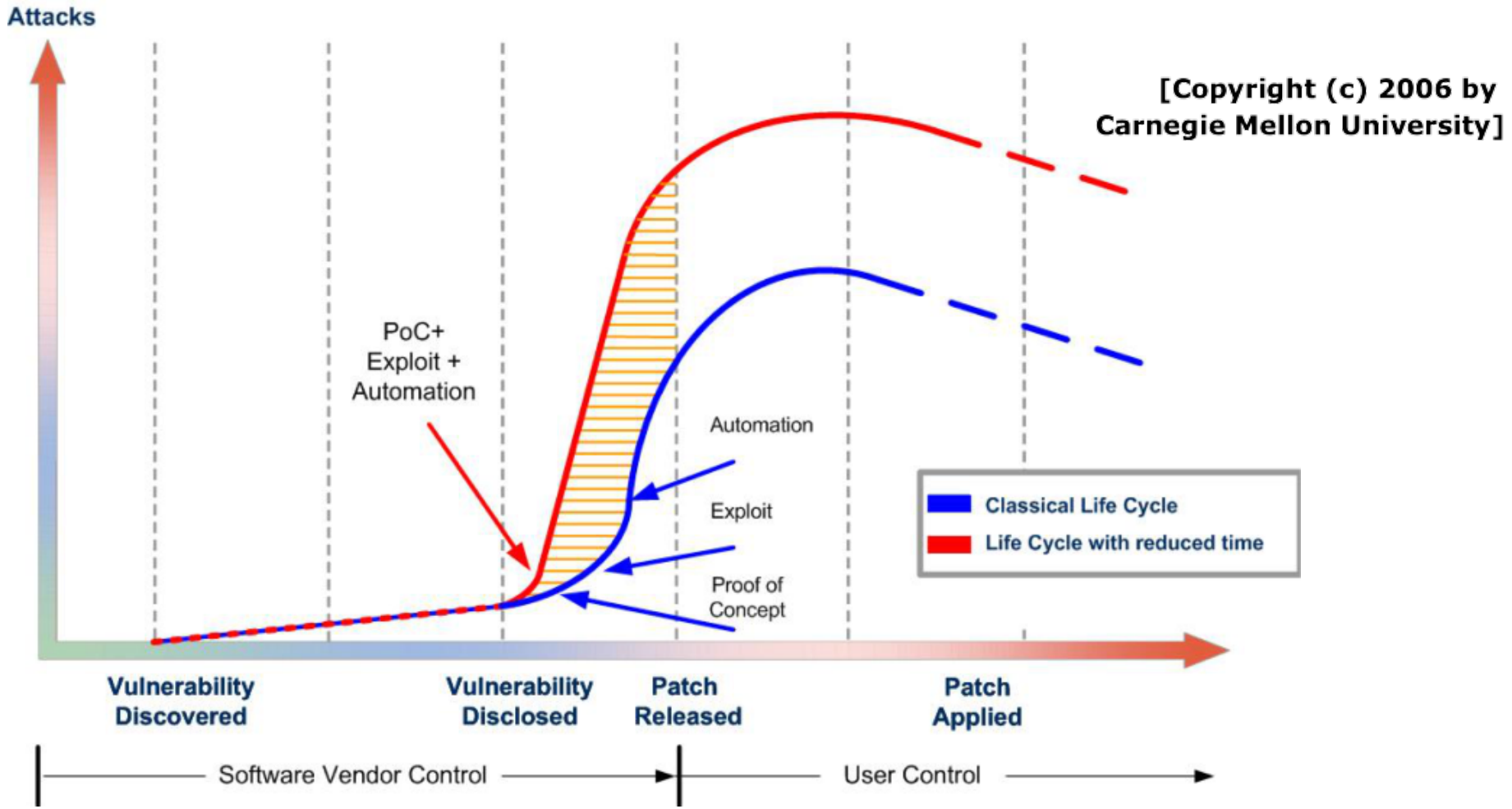
Krisenmanagement etablieren

... Und auch mit den „kleinen“ und „normalen“ Krisen fertig werden!

Ausreichend Ressourcen einsetzen

Technik, Automatisierung, aber immer auch Personal

Eskalierter Lebenszyklus



Was muss das Management gewährleisten?

- **Es muss „strategisches Lernen“ der eigenen Organisation ermöglichen!**
  - Mentale Modelle sind stark, müssen aber langsam und beharrlich verändert werden
- **Feedback ist dafür elementar:**
  - Verkürzung der Feedbackphasen
  - Vorwegnehmen des erwarteten Feedbacks
- **Nur eine Veränderung der Kultur einer Organisation ermöglicht echte Verbesserungen!**

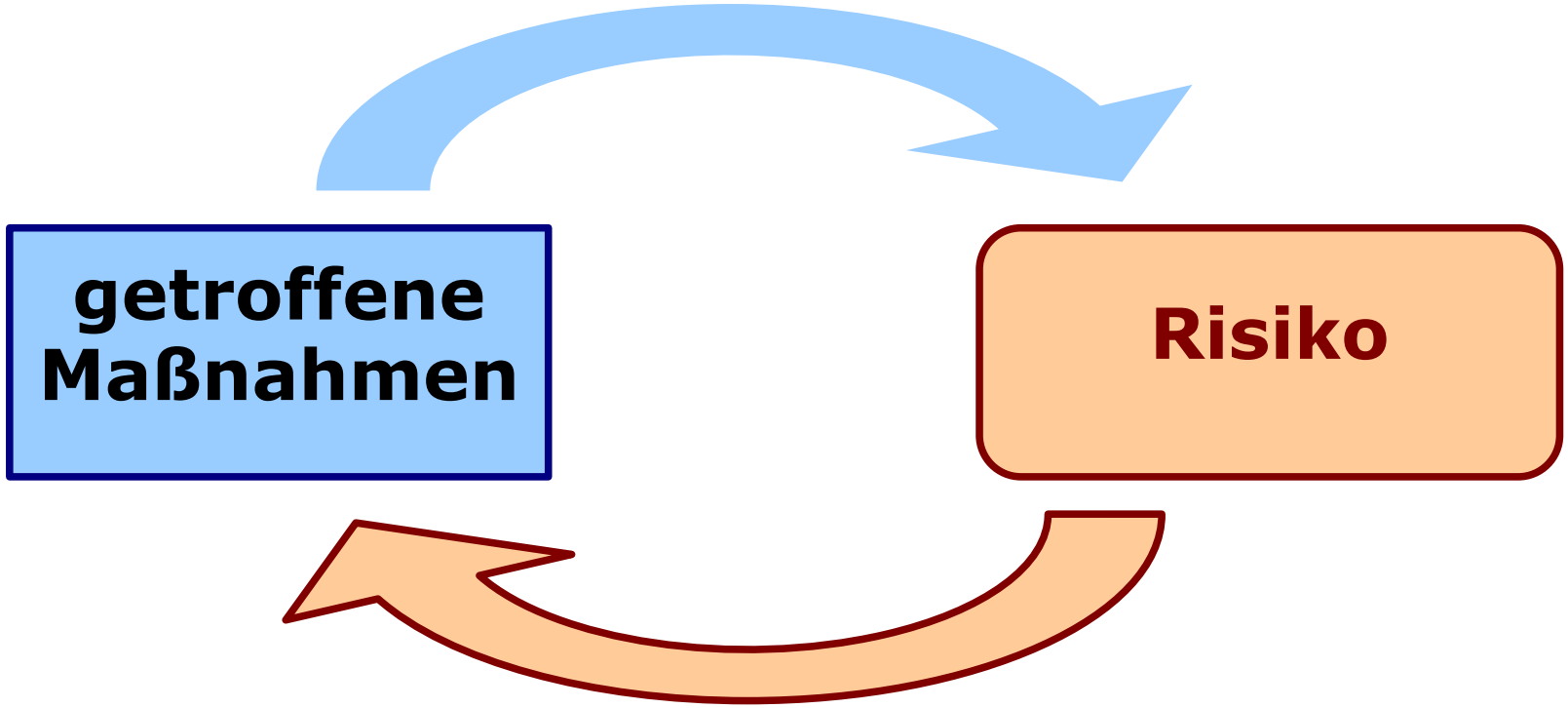
Weiterhin viel zu viele Vorfälle!

- **Eigentlich nimmt die Anzahl von Security Policies (u.ä.) immer weiter zu …**
  - Doch fehlende oder falsche Umsetzungen schließen nicht alle Lücken, die für Angriffe genutzt werden!
- **Eigentlich sollte sich die Code-Qualität deutlich verbessert haben ...**
  - Aber weiterhin beruhen die meisten Exploits auf vermeidbaren Programmierfehlern!

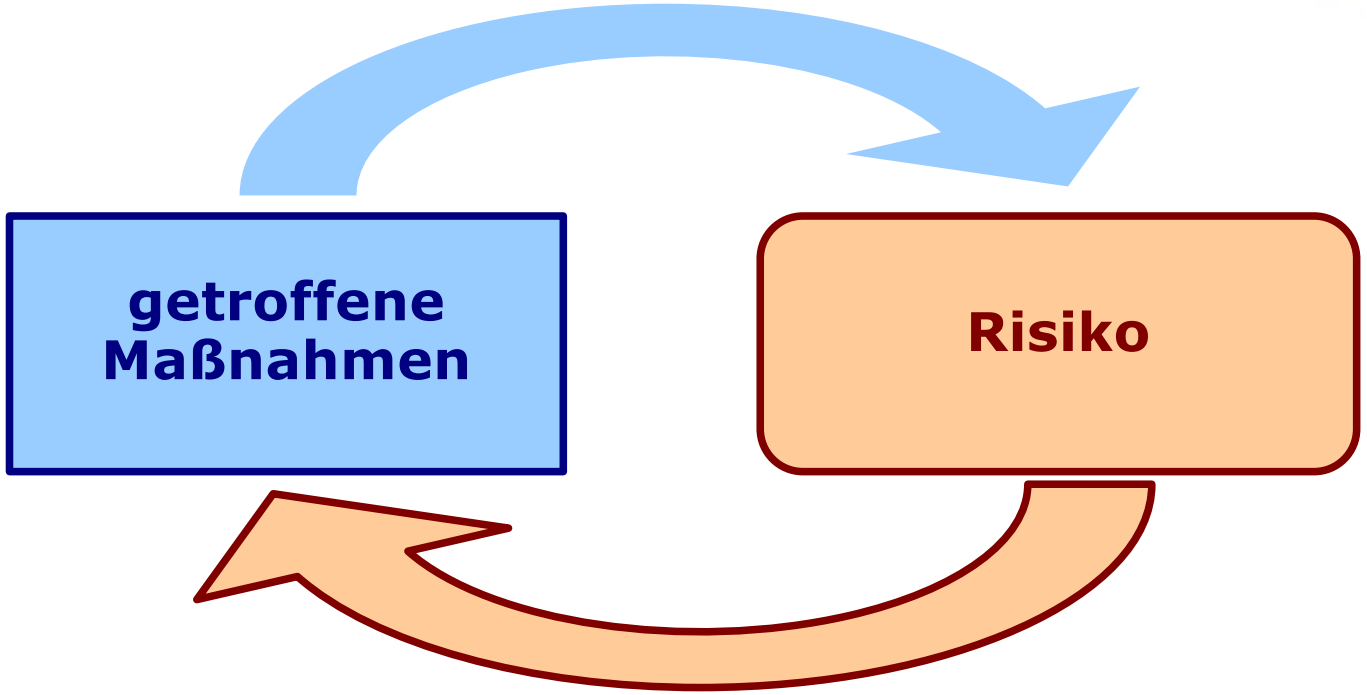
Und die Erkennung klappt auch nicht!

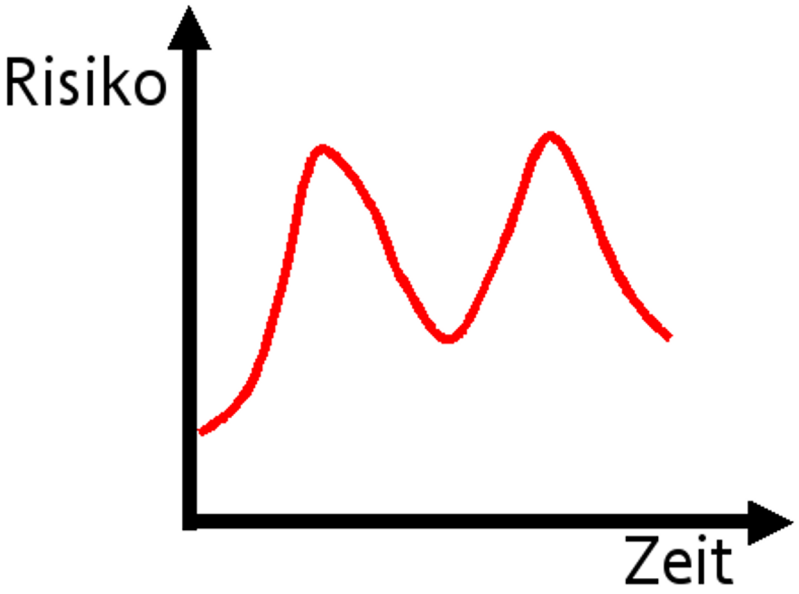
- **Ungeachtet aller Monitoring- und Audit-Aktivitäten vergehen Tage, Wochen oder Monate, bis signifikante Vorfälle aufgedeckt werden!**
- **Und selbst dann fällt es selbst vorbereiteten Organisationen schwer**
  - schnell (genug) und
  - effektiv
- **darauf zu reagieren**

PDCA ist gut .... Hier mal einfacher!



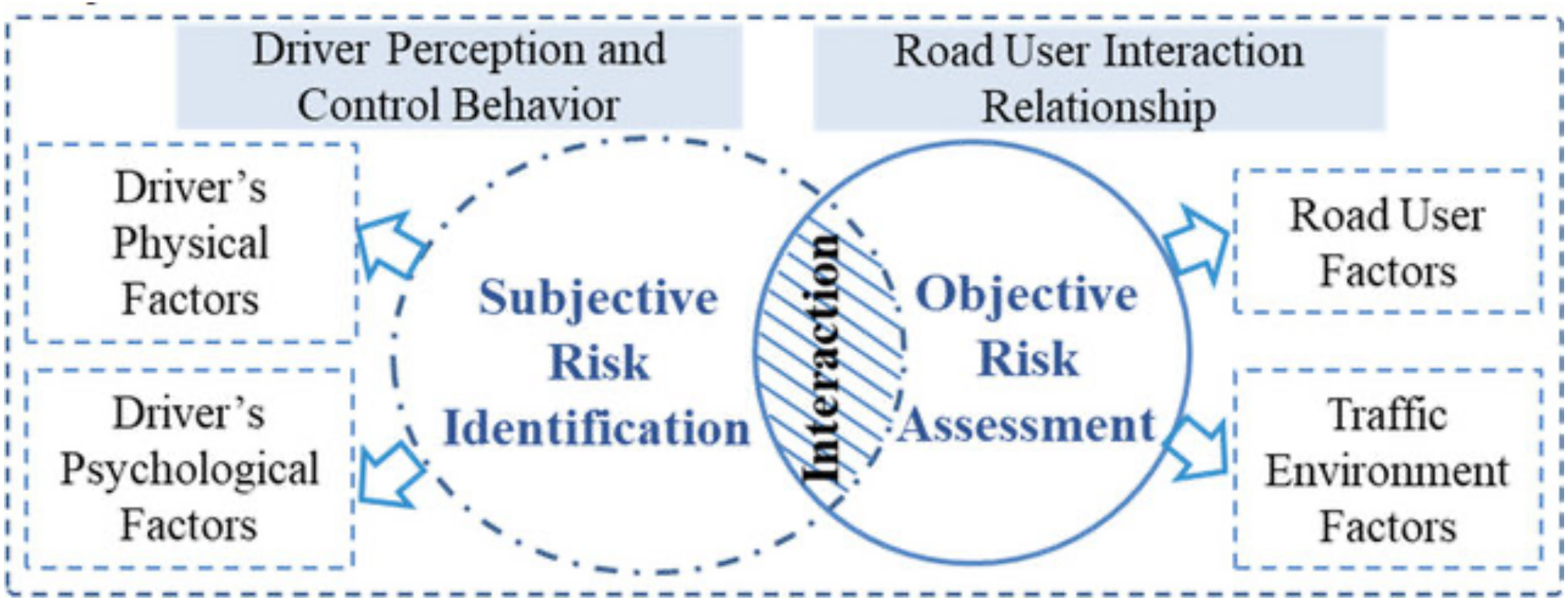
PDCA und dokumentiertes Risiko





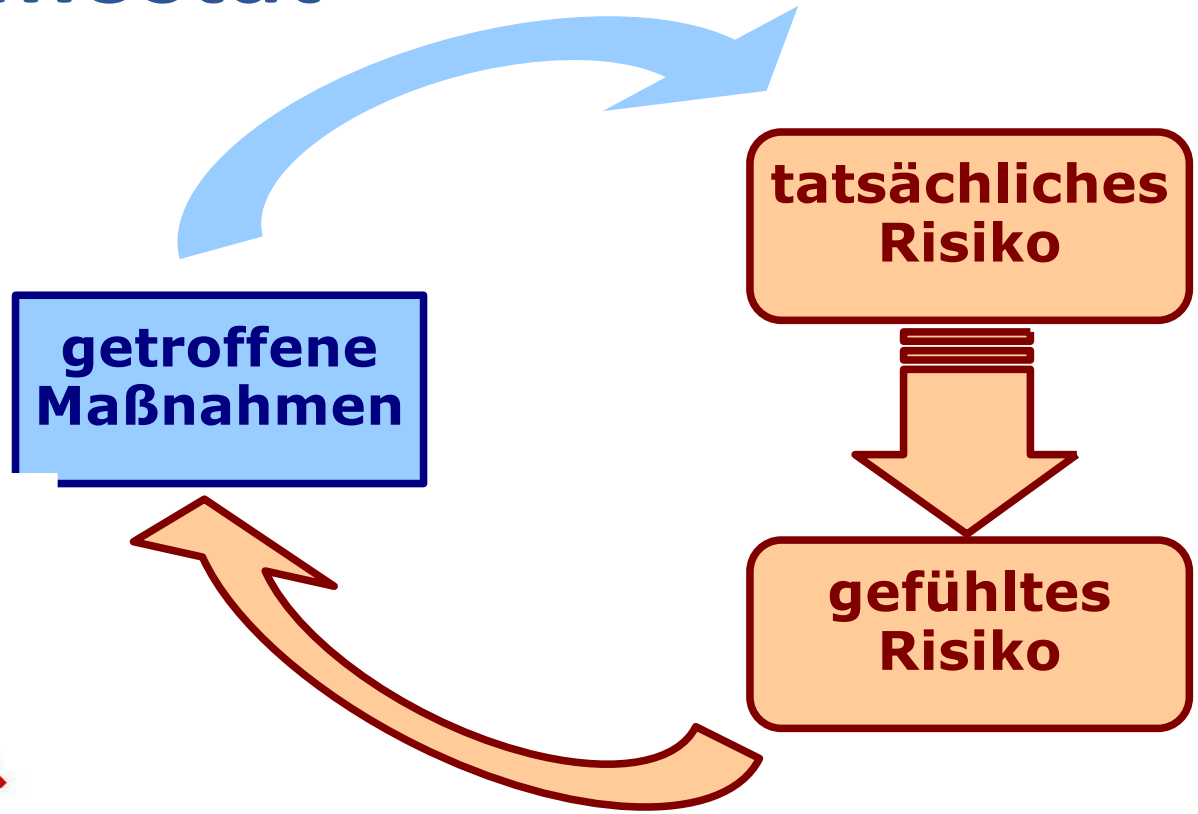
tatsächliches Risiko

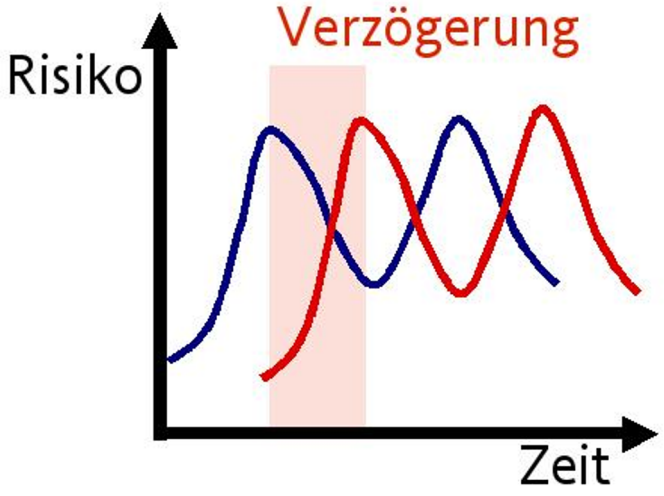
Risikofaktoren werden aber nicht objektiv wahrgenommen!



[Heye et al. 2019] Heye, Huang & Li, Yang & Zheng, Xunjia & Wang, Jianqiang & Xu, Qing & Zheng, Sifa. (2019). Objective and Subjective Analysis to Quantify Influence Factors of Driving Risk *. 4310-4316. 10.1109/ITSC.2019.8917382.

Das Risiko-Thermostat





…feedback mechanisms may provide a systemic limit on the performance of some risk reduction systems

– Anderson (2001 p. 493)

“CIA” reicht ja schon lange nicht mehr!

Aber **Parker's Hexad** auch nicht mehr …

CSIRT Services Framework

- **1st Release als SIRT Services Framework: Juli 2016**
  - In einigen Sprachen durch die ITU übersetzt
  - Verbesserungen durch Version 1.1 im Mai 2017
  - Danach wurde das PSIRT Services Framework gestartet
- **Die neue Version wurde intern als Entwurf im Juli 2019 freigegeben**
  - Gegenüber der Version 1.1 gab es sehr weitreichende Änderungen - sowohl in Struktur als beim Inhalt
- **Veröffentlicht als 2.1 im November 2019**
  - Auch diese Version wird durch die ITU übersetzt werden

→ **https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1**

Was wird jetzt festgelegt?

Die Struktur ergibt sich aus dem Verhältnis von vier Kernbereichen:

SERVICE AREAS

→ SERVICES

→ FUNCTIONS

→ SUB-FUNCTIONS

SERVICE AREA
Information Security Event Management

SERVICE AREA
Information Security Incident Management

SERVICE AREA
Vulnerability Management

SERVICE AREA
Situational Awareness

SERVICE AREA
Knowledge Transfer

SERVICE AREAS

- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support

Information Security Incident Management

- Vulnerability Discovery/Research
- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Coordination
- Vulnerability Disclosure
- Vulnerability Response

Vulnerability Management

- Monitoring and Detection
- Event Analysis

Information Security Event Management

- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

Knowledge Transfer

- Data Acquisition
- Analysis and Synthesis
- Communication

Situational Awareness

Anwendbar auf viele unterschiedliche Teams

- Qual der Wahl für Product Security Incident Response Teams (PSIRTs), weil es dafür ein eigenes Service Framework gibt
- In unserer (die der FIRST SIG) weiteren Arbeit wird es um Rollen und Kompetenzen gehen, die ebenfalls bisher kaum vernünftig beschrieben oder erklärt werden
- Und der Kommunikation von Maturity Leveln wird mehr und mehr an Bedeutung gewinnen

Version 12 October 2020	Service Area: Information Security Incident Management																								
	Report Acceptance			Incident Analysis					Evidence Analysis				Mitigation and Recovery				Information Security Incident Coordination						Crisis Mgmt Support		
Role Name	Information Security Incident Report Receipt	Information Security Incident Triage and Processing	Information Security Incident Report Handling	Information Security Incident Triage (Prioritization and Categorization)	Information Collection	Detailed Analysis Coordination	Information Security Incident Root Cause Analysis	Cross-Incident Correlation	Media or Surface Analysis	Reverse Engineering	Runtime or Dynamic Analysis	Comparative Analysis	Response Plan Establishment	Ad Hoc Measures and Containment	System Restoration	Other Information Security Entities Support	Communication	Notification Distribution	Relevant Information Distribution	Activities Coordination	Reporting	Media Communication	Information Distribution to Constituents	Information Security Status Reporting	Strategic Decisions Communication
Incident Analyst							x	x	x																
Incident Triage Coordinator	x	x	x	x																				x	
Incident Responder					x	x							x	x		x	x	x	x	x	x				
Malware / Forensic Analyst								x	x	x	x	x													
IT Administrator															x										
Communication Liaison																						x	x		x

Auszug aus dem neuen Working Draft der FIRST SIG „CSIRT Framework Development“ (2020)

Maturity

How effectively an organization executes a particular capability within the mission and authorities of the organization. It is a level of proficiency attained either in executing specific functions or in an aggregate of functions or services. The ability of an organization will be determined by the extent and quality of established policies and documentation and the ability to execute a set process.

→ **https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1**

Maturity, aber Capacity und Capabilities zuerst

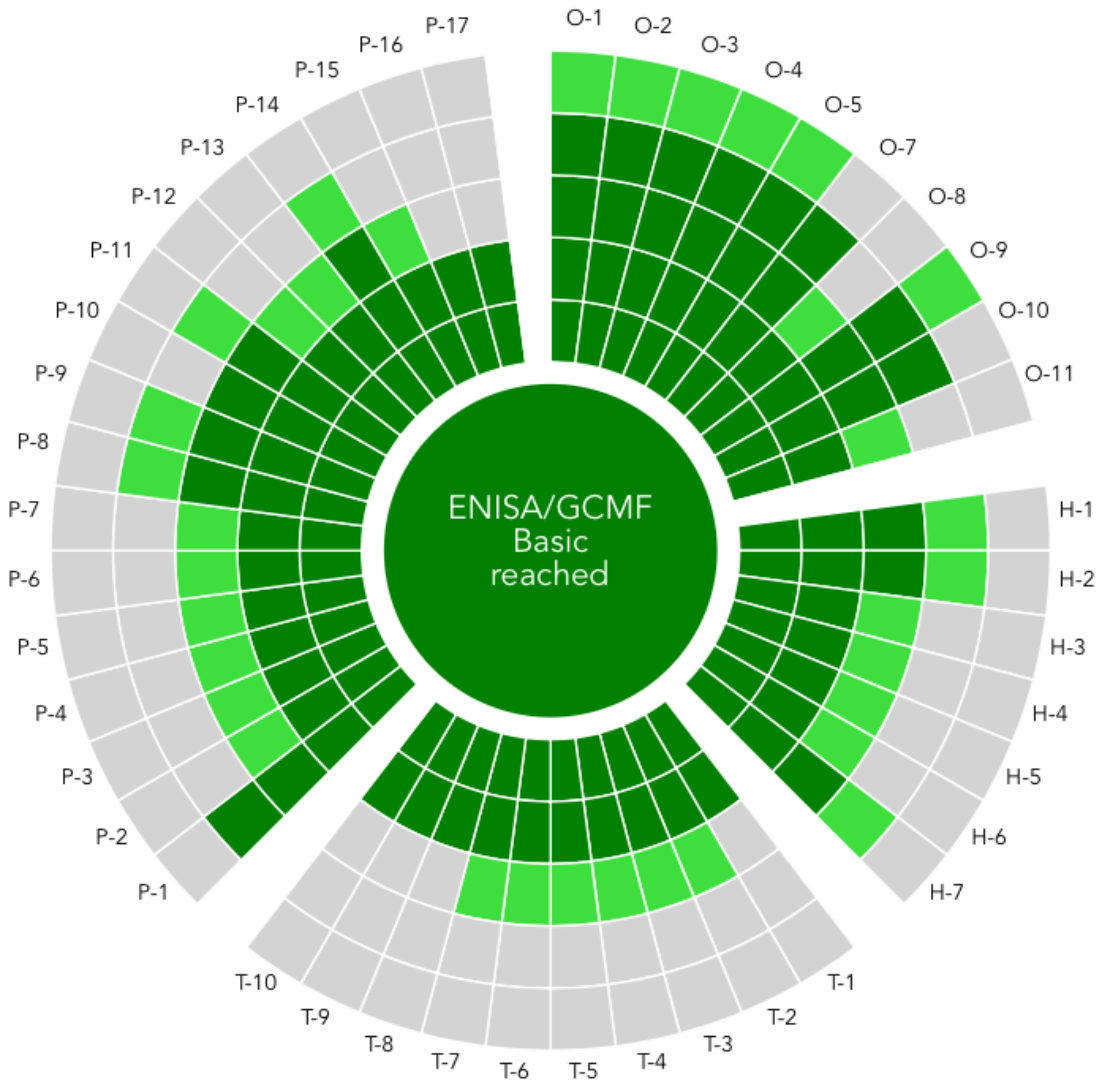
- **Capability -** A measurable activity that may be performed as part of an organization's roles and responsibilities. For the purposes of the FIRST services framework, the capabilities can either be defined as the broader services or as the requisite functions.

- **Capacity -** The number of simultaneous process-occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

→ **https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1**

Wie bewerten wir nun die “Reife” (Maturity)?

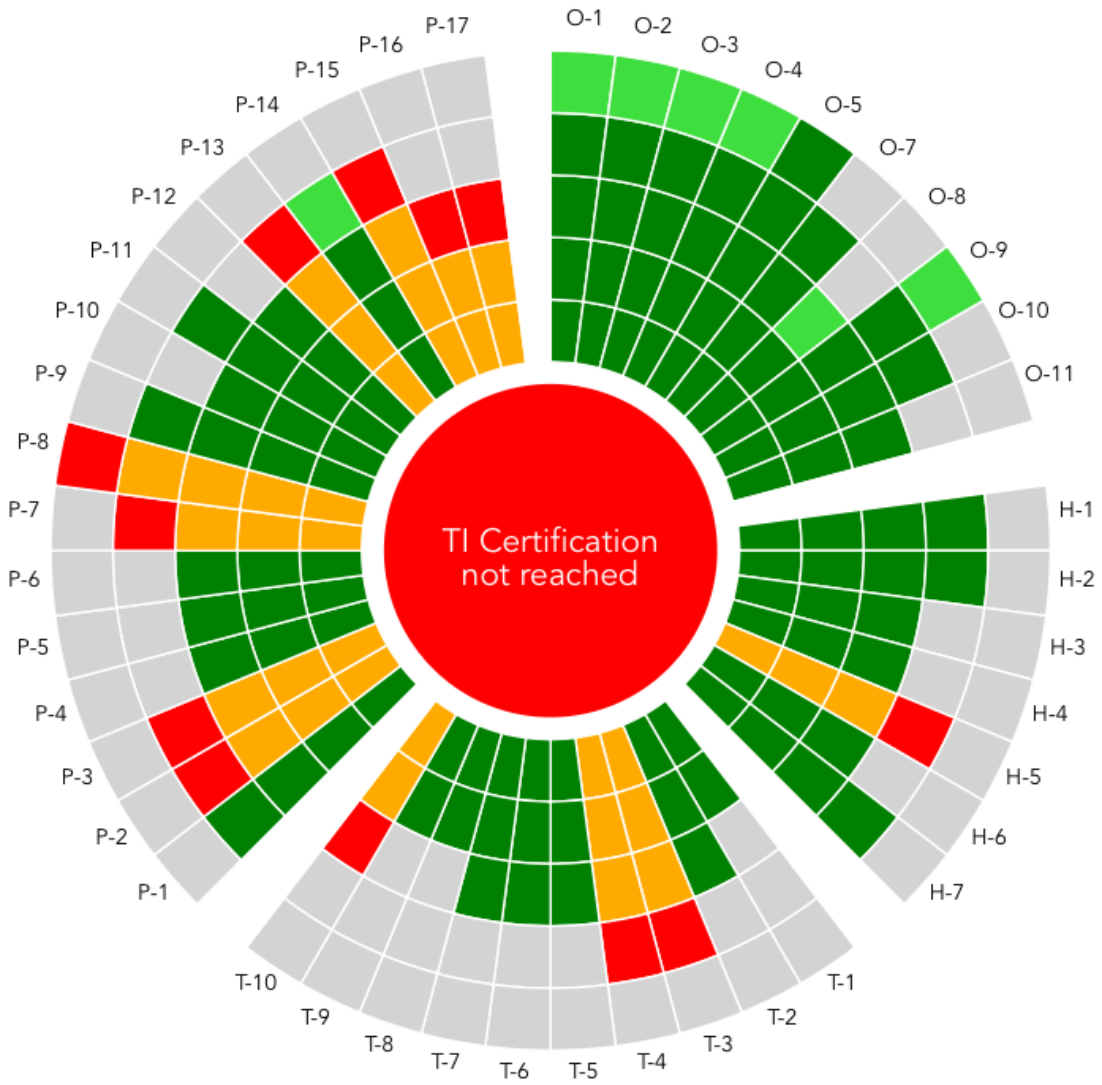
- **Organisation** –
  Mandate, Zuständigkeit, Policies
- **Human Issues** –
  Personal und Ausbildung
- **Prozesse** –
  Ablauforganisation und Maßnahmen
- **Technologie** –
  Werkzeuge und Lösungen



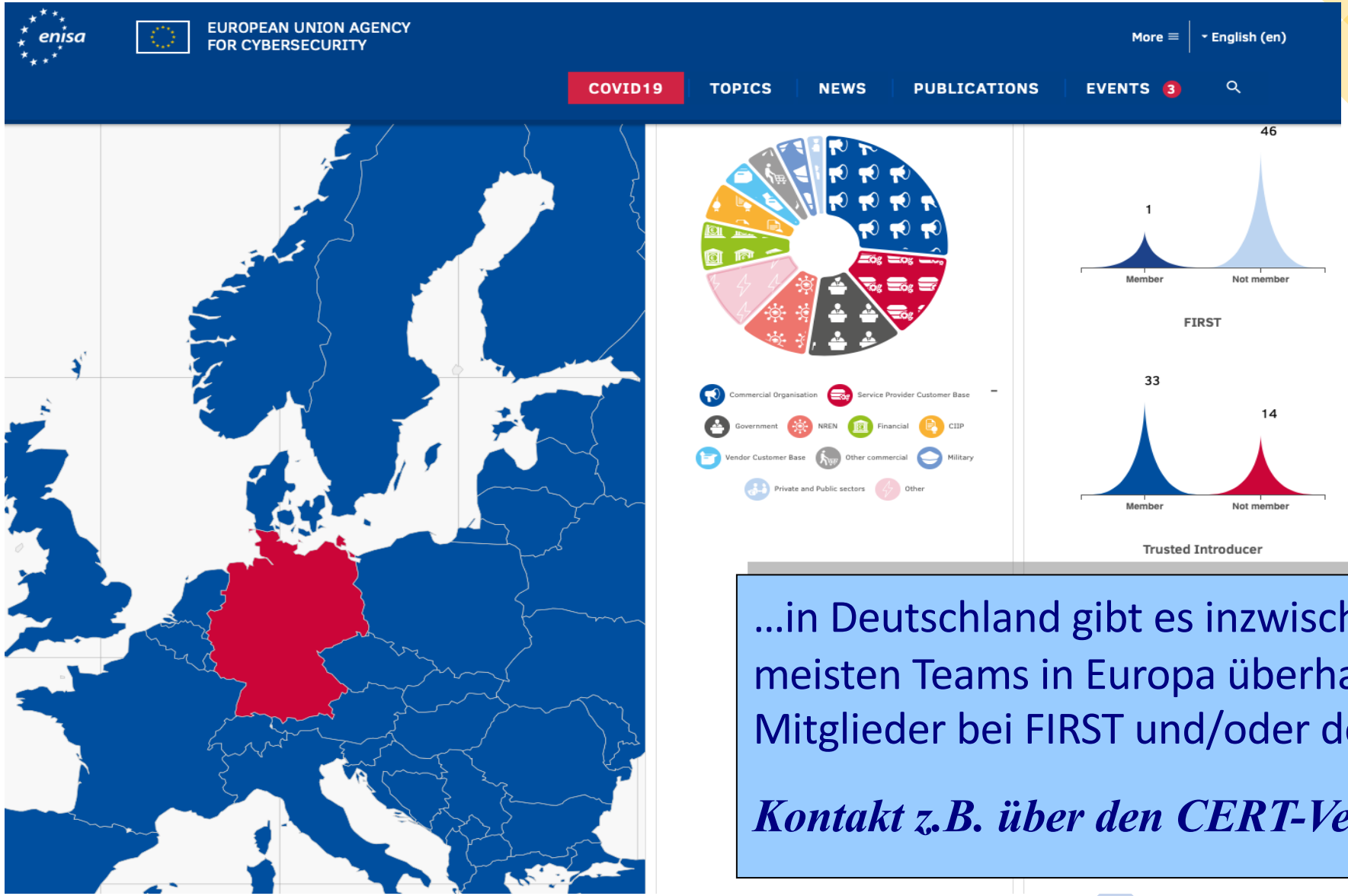
https://sim3-check.opencsirt.org/#/v1/6CaesRqXY-5DCmaSzGi-BxRFXmVh

Wie bewerten wir nun die “Reife” (Maturity)?

- **Organisation** –
  Mandate, Zuständigkeit, Policies
- **Human Issues** –
  Personal und Ausbildung
- **Prozesse** –
  Ablauforganisation und Maßnahmen
- **Technologie** –
  Werkzeuge und Lösungen



https://sim3-check.opencsirt.org/#/v1/6CaesRqXY-5DCmaSzGi-BxRFXmVh



…in Deutschland gibt es inzwischen mit die meisten Teams in Europa überhaupt. Viele sind Mitglieder bei FIRST und/oder der TF-CSIRT!

Kontakt z.B. über den CERT-Verbund!

https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Germany

Advisories

Unsere Advisories sind ausschließlich in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Datum	ID	Titel
2020-10-27	VDE-2020-031	ENDRESS+HAUSER: Products utilizing WIBU-SYSTEMS AG Code Meter component
2020-10-27	VDE-2020-042	WAGO: PLC families 750-88x and 750-352 prone to DoS attack, versions < FW10
2020-10-27	VDE-2020-039	TRUMPF: Multiple products prone to WIBU CodeMeter vulnerabilities
2020-10-16	VDE-2020-043	BENDER: COMTRAXX - Inadequate credentials check
2020-09-30	VDE-2020-027	WAGO: Vulnerability in web-based authentication in WAGO 750-8XX Version
2020-09-18	VDE-2020-035	MB connect line: Multiple Vulnerabilities in mymbCONNECT24 and mbCONNECT24 <= v2.6.1

RSS Feeds

Atom

RSS

…in Deutschland ist eine Europaweit-führende Initiative für die Automatisierungsindustrie das VDE-CERT!

https://cert.vde.com/de-de

Kontakt

Prof. Dr.
Klaus-Peter Kossakowski

klaus-peter.Kossakowski
@haw-hamburg.de

+49 171 5767010

Aktuelles Projekt: Schwerpunkt ”Sicherheit und Zuverlässigkeit” im Master Informatik:
http://users.informatik.haw-hamburg.de/~kpk/ms-s-und-z.html