Cybersicherheit als Fundament der digitalen Souveränität

Einblicke ins CSAFversum: Cyber-Resilienz proaktiv gestalten

Bundesamt
für Sicherheit in der
Informationstechnik

Bild: © AdobeStock/Nirut

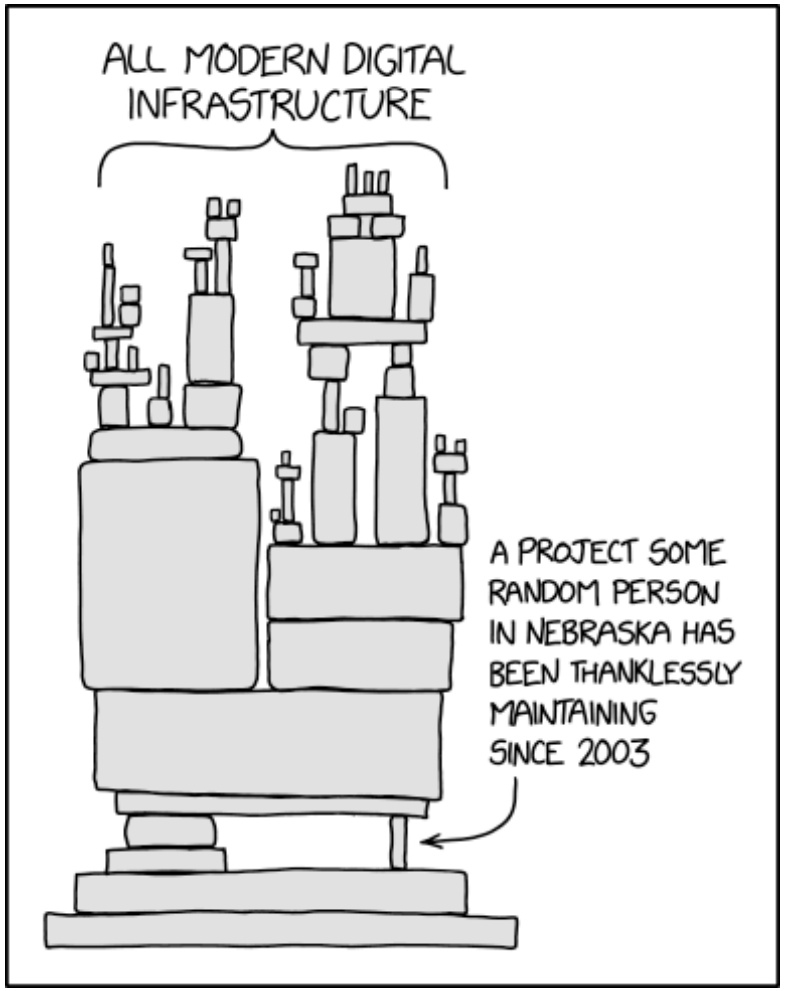
Ich hab ein Haus, ein Äffchen und ein Pferd…

Bild: © AdobeStock/Azazul

Ich hab n Produkt, ne Schwachstelle und ein Problem…

Die Realität der digitalen Souveränität

- Zunehmende **Digitalisierung** und **Vernetzung**
- Viele **Abhängigkeiten**
- **Usability** und **Datensicherheit**

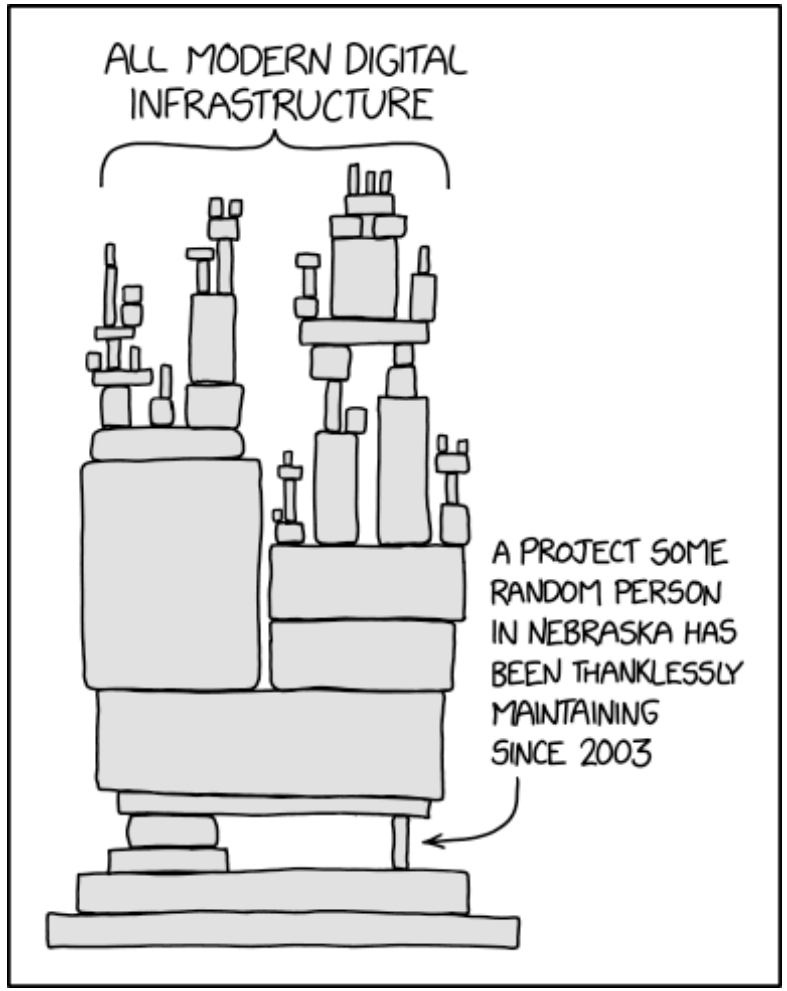


https://xkcd.com/2347/

Ich hab n Produkt, ne Schwachstelle und ein Problem…

Die Realität der digitalen Souveränität

- Zunehmende **Digitalisierung** und **Vernetzung**
- Viele **Abhängigkeiten**
- **Usability** und **Datensicherheit**
- **Verantwortlichkeiten?**
- **Sichere Lieferkette(n)?**

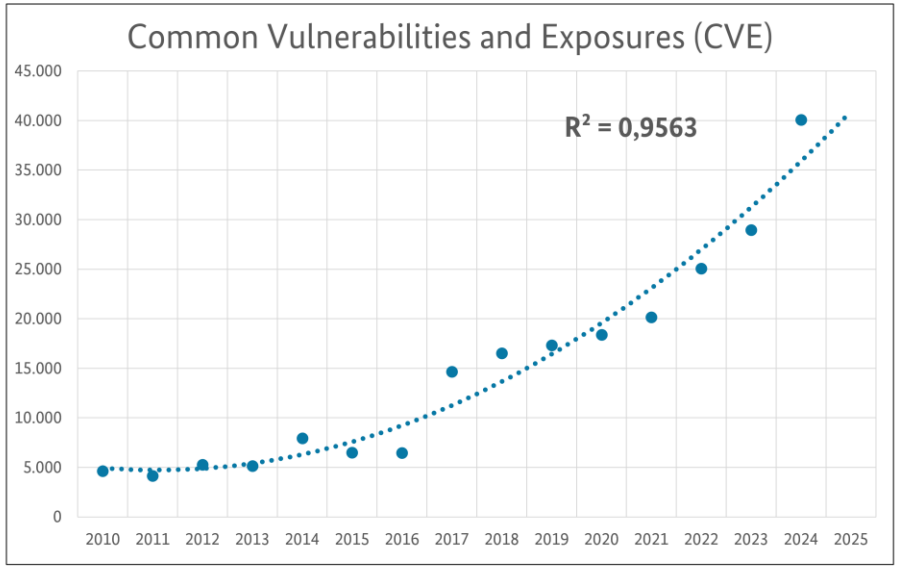


https://xkcd.com/2347/

Sicherheitsinformationen in Form von Security Advisories

Woher bekomme ich meine Informationen?

- **Anzahl sicherheitsrelevanter Schwachstellen steigt**
- **Viele Quellen** (Hersteller, Behörde, etc.)
- **Unterschiedliche Übertragungswege** (Mail, Feed, Webseite, etc.)
- **Diverse Formate** (.pdf, .txt, .html, etc.)

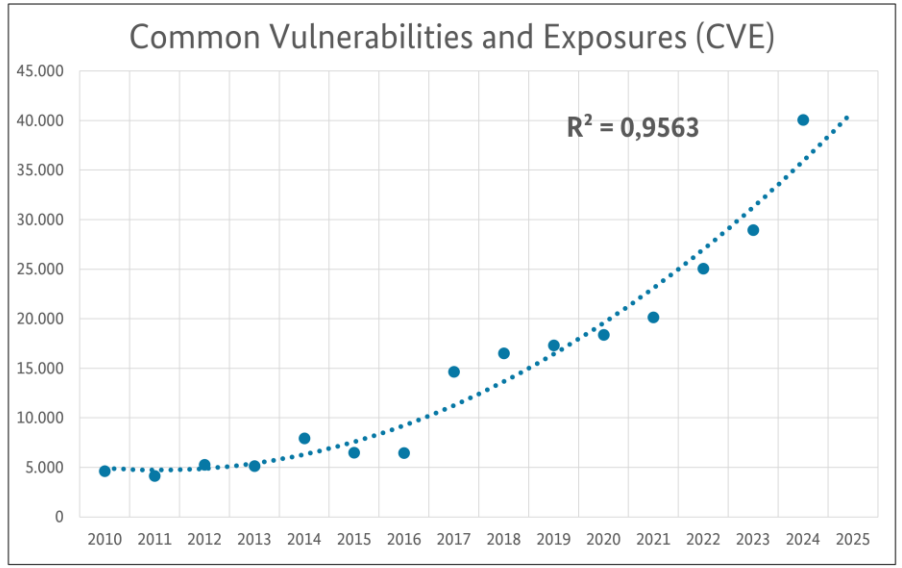


Jahr	Anzahl der CVE
2010	4.639
2011	4.150
2012	5.288
2013	5.142
2014	7.948
2015	6.494
2016	6.457
2017	14.645
2018	16.512
2019	17.308
2020	18.375
2021	20.161
2022	25.059
2023	28.961
2024	40.077

Sicherheitsinformationen in Form von Security Advisories

Woher bekomme ich meine Informationen?

- **Anzahl sicherheitsrelevanter Schwachstellen steigt**
- **Viele Quellen** (Hersteller, Behörde, etc.)
- **Unterschiedliche Übertragungswege** (Mail, Feed, Webseite, etc.)
- **Diverse Formate** (.pdf, .txt, .html, etc.)
- **Manueller Abgleich** mit den eigenen Systemen und der eigenen Infrastruktur
- **Manuelle Bewertung** (Kritikalität, Betroffenheit, etc.)



Jahr	Anzahl der CVE
2010	4.639
2011	4.150
2012	5.288
2013	5.142
2014	7.948
2015	6.494
2016	6.457
2017	14.645
2018	16.512
2019	17.308
2020	18.375
2021	20.161
2022	25.059
2023	28.961
2024	40.077

Der CRA in Daten und Fakten

11.12.2024

Der CRA tritt in Kraft

11.06.2026

Konformitätsbewertungs-stellen können die Erfüllung der Anforderungen an den CRA bewerten

11.09.2026

Meldepflicht für Schwachstellen und Sicherheitsvorfälle

11.12.2027

Alle CRA-Anforderungen sind bei neuen Produkten eingehalten

Starten Sie mit der security.txt (RFC9116)

Menschen- und maschinenlesbare Kontaktinformation

```
# Our security address
Contact: mailto:security@example.com
Contact: mailto:productsecurity@example.com
Contact: https://example.com/security/contact.html
Contact: tel:+49-69-9000-9116

# Our OpenPGP key
Encryption: https://example.com/security/pgp-key.asc

# Our security acknowledgments
Acknowledgments: https://example.com/security/hall-of-fame.html

# Our preferred languages
Preferred-Languages: en, de, fr, nl, es

# Our security policy
Policy: https://example.com/security/disclosure-policy.html
```

Starten Sie mit der security.txt (RFC9116)

Menschen- und maschinenlesbare Kontaktinformation

- Datei mit **relevanten Kontaktinformationen** einer Organisation
- Befindet sich an einem **definierten Ort** auf der Internetseite
- **Vereinfacht Kontaktaufnahme** mittels automatischer Werkzeuge
- **Organisation geht IT-Sicherheit proaktiv an**

```
# Our security address
Contact: mailto:security@example.com
Contact: mailto:productsecurity@example.com
Contact: https://example.com/security/contact.html
Contact: tel:+49-69-9000-9116

# Our OpenPGP key
Encryption: https://example.com/security/pgp-key.asc

# Our security acknowledgments
Acknowledgments: https://example.com/security/hall-of-fame.html

# Our preferred languages
Preferred-Languages: en, de, fr, nl, es

# Our security policy
Policy: https://example.com/security/disclosure-policy.html
```

CSAF – Common Security Advisory Framework

CSAF 2.0 seit 11.2022 internationaler Standard der OASIS, seit 02.2025 ISO-Standard

- **Maschinenlesbares, herstellerunabhängiges** Format für Security Advisories (JSON)
- **Open Source** (OS) und OS Tools verfügbar
- **Standardisiertes** Format und standardisierte Verteilung der Information
- **Automatisierbarer** Publikations-, Verteil- und Abrufmechanismus

CSAF – Common Security Advisory Framework

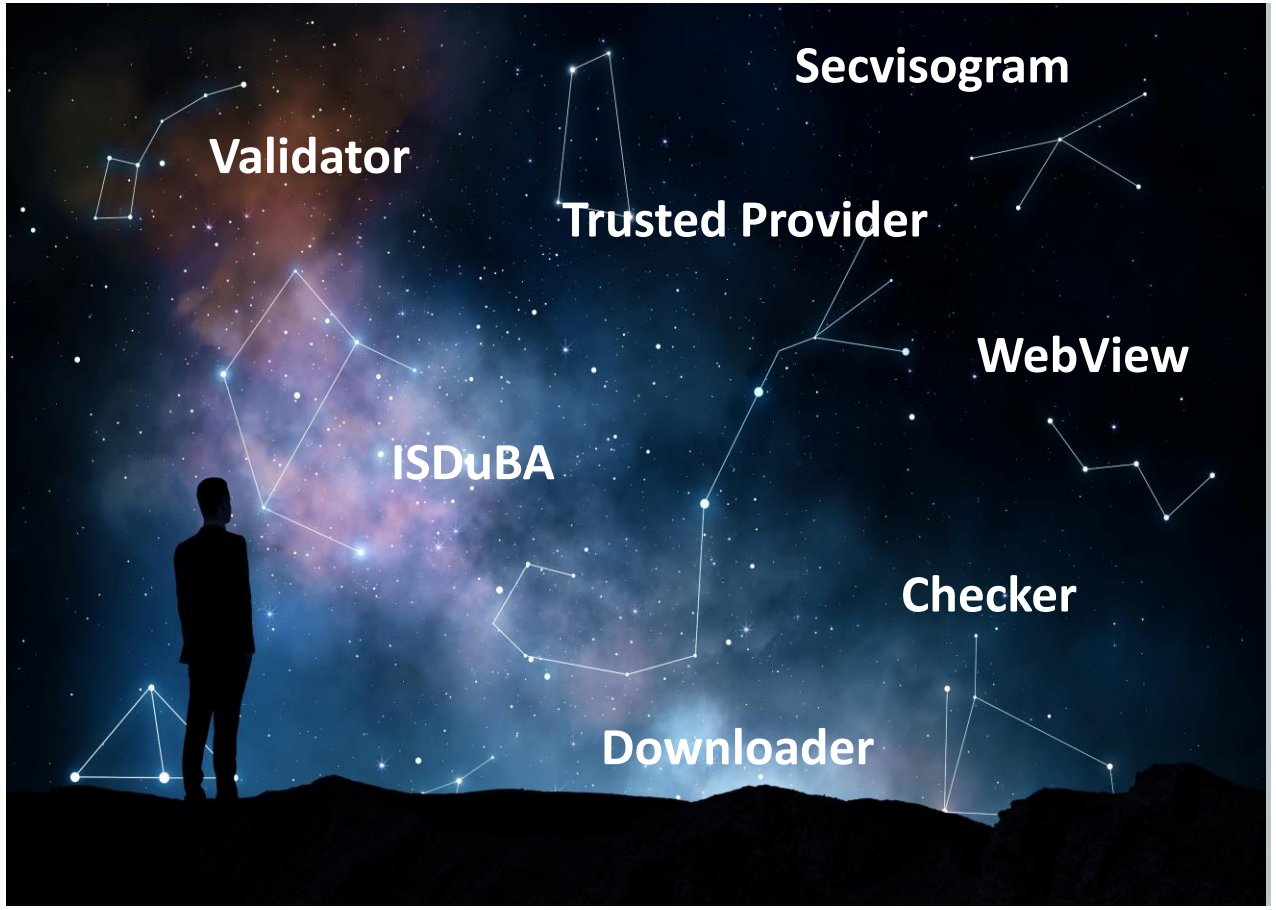
CSAF 2.0 seit 11.2022 internationaler Standard der OASIS, seit 02.2025 ISO-Standard

- **Maschinenlesbares, herstellerunabhängiges** Format für Security Advisories (JSON)
- **Open Source** (OS) und OS Tools verfügbar
- **Standardisiertes** Format und standardisierte Verteilung der Information
- **Automatisierbarer** Publikations-, Verteil- und Abrufmechanismus
- Abgleich mit **Asset Management** und **SBOMs** möglich
- Benachrichtigungen über **verfügbare Sicherheitsupdates und Inhalte**

Das CSAFversum expandiert

CSAF fordern und fördern

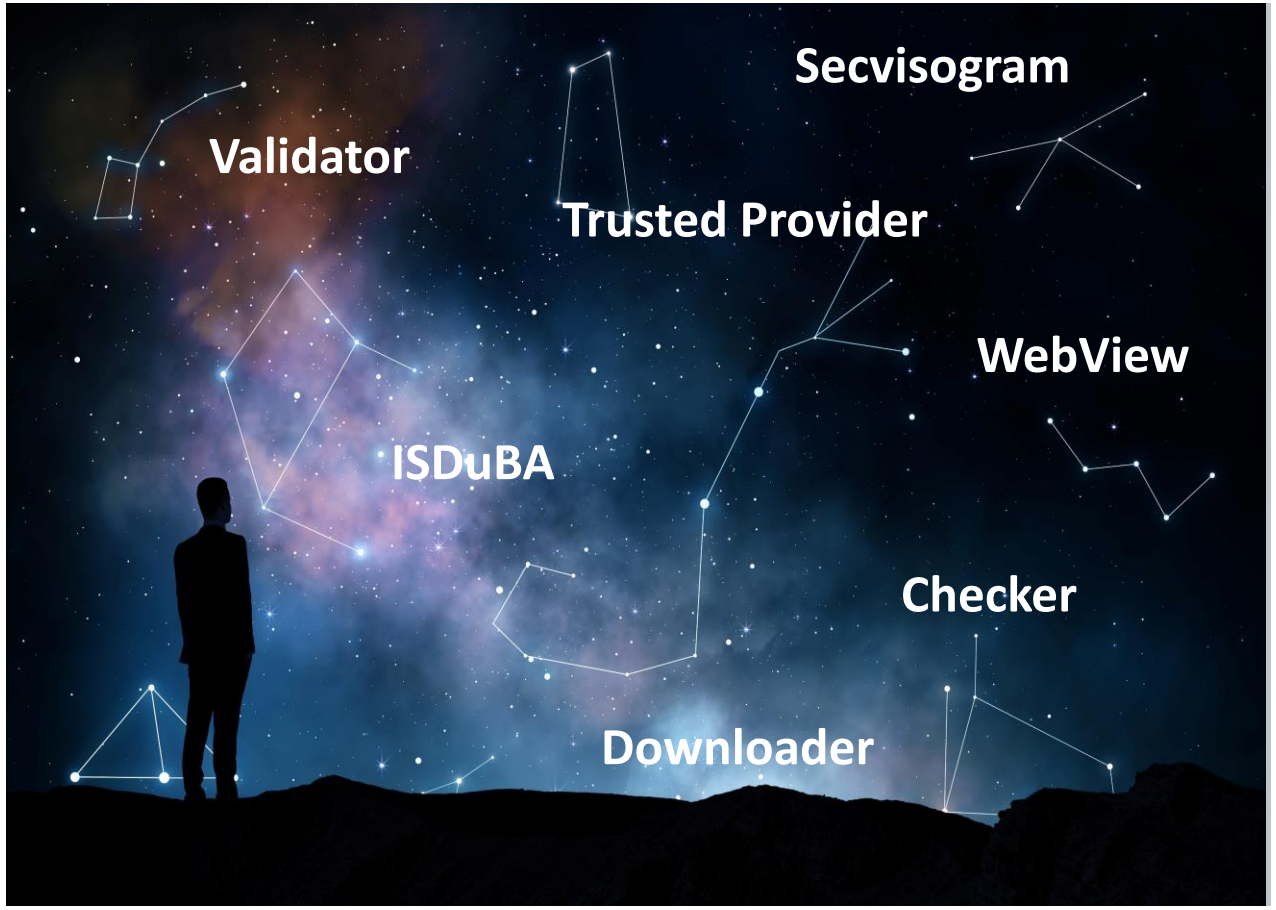
- **CSAF wird genutzt und eingefordert**
- **Open Source Tools** werden weiterentwickelt
- **Synergien** zwischen einzelnen Tools



Das CSAFversum expandiert

CSAF fordern und fördern

- **CSAF wird genutzt und eingefordert**
- **Open Source Tools** werden weiterentwickelt
- **Synergien** zwischen einzelnen Tools
- **CSAF 2.1 Standard** in den Startlöchern
- **Awareness** durch Vorträge, Workshops und Publikationen rund um das Thema CSAF



Die Rolle des BSI

Das CSAFversum expandiert durch viele ineinandergreifende Tätigkeiten

- **Aktive Mitarbeit in der Standardisierung**
- **Erstellung & Erprobung von - sowie Initiativen zu Tools, um Einstieg zu erleichtern**
  - Secvisogram
  - ISDuBA
  - Sec-o-simple
  - TR-03191

Die Rolle des BSI

Das CSAFversum expandiert durch viele ineinandergreifende Tätigkeiten

- Aktive Mitarbeit in der Standardisierung
- Erstellung & Erprobung von - sowie Initiativen zu Tools, um Einstieg zu erleichtern
  - Secvisogram
  - ISDuBA
  - Sec-o-simple
  - TR-03191
- **Bereitstellen von Advisories des Warn- und Informationsdienst mittels CSAF**
  - Aggregation von Advisories von Herstellern (CSAF Aggregator des BSI)
  - Pflege der „Gelben Seiten“ für CSAF (CSAF Lister des BSI)
- **Workshops mit Herstellern & Anwendern**

https://www.bsi.bund.de/csaf

csaf@bsi.bund.de

CSAF TO GO

Schenken Sie diesen Punkten Be**ACHT**ung

1. CSAF ist OpenSource, Toolsammlung, Community
2. Standardisiertes, maschinenverarbeitbares Format (JSON)
3. Automatisierbarer Abruf und Verteilung
4. Skalierbarkeit, weniger manueller Aufwand (delegierbar)
5. Betroffenheit einzelner Produkte direkt feststellbar (VEX ist Profil in CSAF)
6. Nur relevante Advisories werden geladen
7. CSAF 2.1 in den Startlöchern
8. Vereinfachtes Risikomanagement

Dr. Dina Truxius

Fachexpertin

dina.truxius@bsi.bund.de

csaf@bsi.bund.de

+49 (0) 228 99 9582 6147

+49 (0) 15120968958

https://bsi.bund.de/csaf

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

Bild: © AdobeStock/Nirut

Links und weiterführende Informationen

- **CSE-149:** https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_149.html
- **CSAF webpage:** https://csaf.io
- **CSAF producer:** https://github.com/secvisogram/secvisogram
- **CSAF producer:** https://github.com/sec-o-simple/
- **CSAF download and evaluation:** https://github.com/ISDuBA/ISDuBA
- **CSAF trusted provider, checker, aggregator and downloader:** https://github.com/gocsaf/csaf
- **BSI TR-03191:** https://www.bsi.bund.de/dok/TR-03191
- **OASIS TC:** https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf
- **CSAF GitHub:** https://github.com/oasis-tcs/csaf
- **More CSAF Tools:** https://oasis-open.github.io/csaf-documentation/tools

Bild: © AdobeStock/ The Little Hut