Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Gesetzliche Anforderungen an die IT-Sicherheit in der Gebäudeautomation

36. GLT-Anwendertagung, Jens Kluge, 12.09.2024

Kurzprofil des BSI

Gründung
01. Januar 1991

217 Mio. Euro
Budget Haushalt 2022

Stellen 2022
1.733 ↗

183
Neue Stellen zum Vorjahr

BSI vor Ort

- Standorte
- Stützpunkte
- Verbindungsstellen

Darüber hinaus engagiert sich das BSI seit langem intensiv im internationalen und nationalen Rahmen, unter anderem in enger Zusammenarbeit mit bilateralen Partnern sowie in multilateralen Handlungsfeldern rund um EU und NATO.

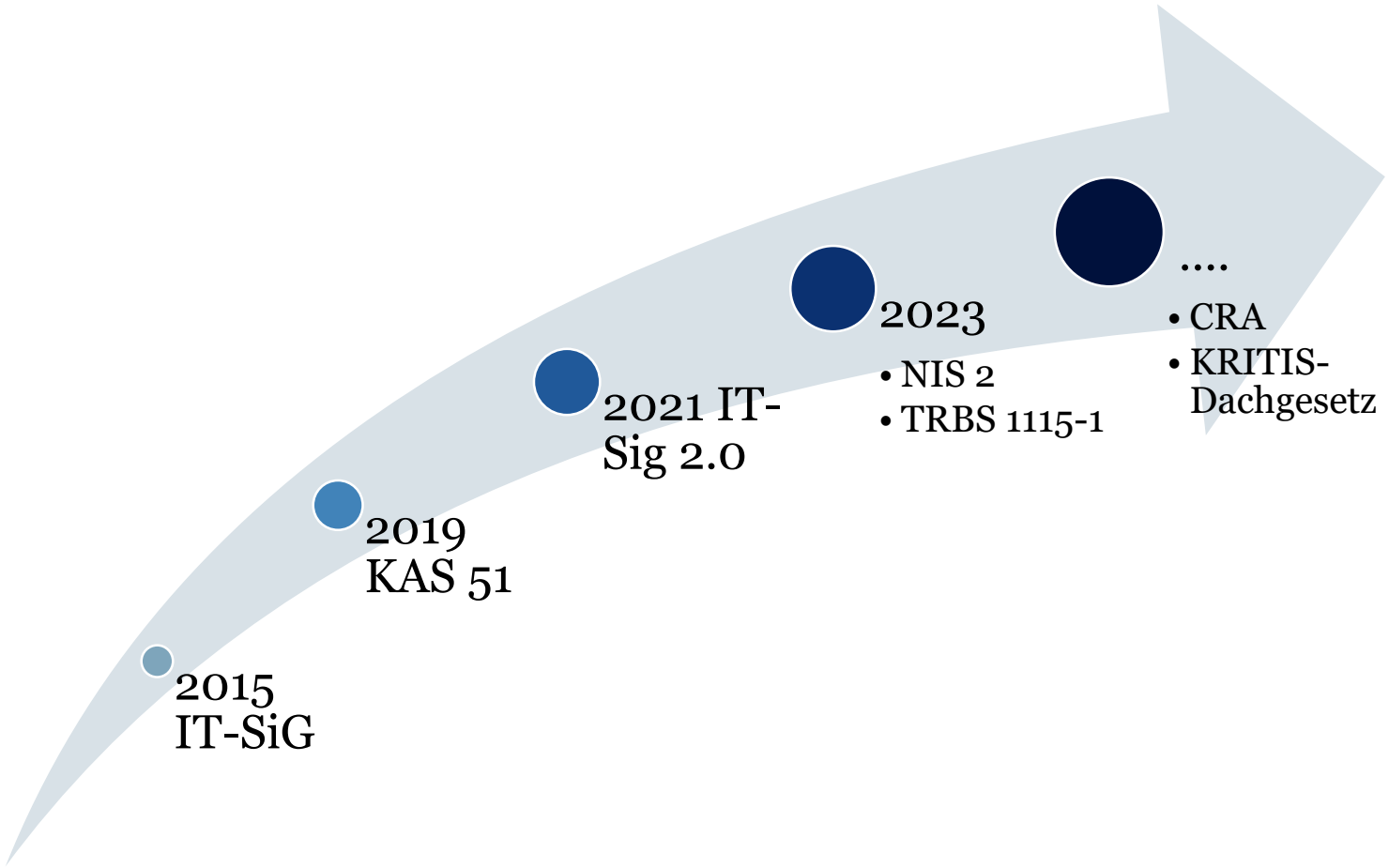
Wie bedroht ist Deutschlands Cyberraum?

- **Ransomware** ist weiterhin die größte Bedrohung.
- Vermehrt wurden **kleine und mittlere Unternehmen (KMU) sowie Kommunalverwaltungen und kommunale Betriebe** angegriffen.
- Mehr als **zwei erfolgreiche Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden im Durchschnitt **in jedem Monat** bekannt.
- Außerdem hat das BSI den **Ausbau einer Schattenwirtschaft** cyberkrimineller Arbeitsteilung beobachtet.

Wie bedroht ist Deutschlands Cyberraum?

- Täglich wurde durchschnittlich rund eine Viertelmillion **neue Schadprogrammvarianten** entdeckt.
- Mehr als 2.000 **Schwachstellen in Softwareprodukten** (15 % davon kritisch) wurden durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24** %.
- **Russischer Angriffskrieg gegen die Ukraine**:
  Im Berichtszeitraum kam es zu einer Reihe pro-russischer Hacktivismus-Angriffe in Deutschland. Diese sind als Propaganda zu werten mit der Absicht, Verunsicherung zu stiften.

Pflichten zur Cybersicherheit steigen



Cyber Resilence Act (CRA)

- Sichere Produkte über den gesamten Lebenszyklus
- SBOM (Software Bill of Materials)
- Schwachstellenmanagement
- → CRA als Teil des “New Legislative Framework” erweitert die Gesetzgebung von reiner Produktsicherheit (Safety) um Security

Cyber Resilence Act (CRA)

- **BSI TR-03183** Cyber-Resilienz-Anforderungen an Hersteller und Produkte
  - In Teil 1 "Allgemeine Anforderungen"
    - Anforderungen an Hersteller und Produkte in Anlehnung an die Anforderungen aus Artikeln und Anhang des CRA zusammengestellt.
    - Teil 1 wird aktuell erarbeitet.
  - Teil 2 "Software Bill of Materials (SBOM)“
    - formelle und fachliche Vorgaben für SBOMs beschrieben, die u. a. in Teil 1 der TR-03183 gefordert werden
    - Teil 2 durch BSI veröffentlicht

NIS 2 Direktive

- 2022 auf EU-Ebene in Kraft getreten
- Bis Oktober 2024 in nationales Recht umzusetzen

Hinweis: Aussagen zur NIS2 beziehen sich auf die EU-Richtlinie, da das nationale Umsetzungsgesetz noch nicht vorhanden ist.

Wesentliche Einrichtungen

- Unternehmen mit
  - >= 250 Beschäftigte oder
    > 50 Mio. € Umsatz und > 43 Mio. € Bilanz
- aus den Sektoren *
  - Verkehr
  - Bankwesen / Finanzmarktinfrastrukturen
  - Gesundheitswesen
  - Trinkwasser / Abwasser
  - Energie
  - Digitale Infrastruktur / Verwaltung von IKT-Diensten (B2B)
  - öffentliche Verwaltung
  - Weltraum

* weitere Sonderfälle/Sektoren können national ergänzt werden

Proaktive Aufsicht durch Einfordern von Nachweisen oder Audits

Wichtige Einrichtungen

- Unternehmen mit
  - > 50 und < 250 Beschäftigte oder
    > 10 Mio. € und < 50 Mio. € Umsatz
- aus den Sektoren *
  - Verkehr
  - Bankwesen / Finanzmarktinfrastrukturen
  - Gesundheitswesen
  - Trinkwasser / Abwasser
  - Energie
  - Digitale Infrastruktur / Verwaltung von IKT-Diensten (B2B)
  - öffentliche Verwaltung
  - Weltraum

- Unternehmen mit
  > 50 Beschäftigte, oder
  > 10 Mio. EUR Umsatz und Bilanz

- aus den Sektoren *
  - Abfallbewirtschaftung
  - Produktion, Herstellung und Handel mit chemischen Stoffen
  - Produktion, Verarbeitung und Vertrieb von Lebensmitteln
  - Verarbeitendes Gewerbe/Herstellung von Waren
  - Anbieter digitaler Dienste
  - Post- und Kurierdienste
  - Forschung

* weitere Sonderfälle/Sektoren können national ergänzt werden

Reaktive Aufsicht nach Hinweisen auf Verstöße durch Nachweise oder Audits

Pflichten für wesentliche und wichtige Einrichtungen

- Maßnahmen zum Risikomanagement für Cybersicherheit umsetzen
  - Konzepte für Risikoanalyse und Sicherheit für Informationssysteme
  - Prävention, Erkennen und Bewältigen von Sicherheitsvorfällen
  - Bewerten der Wirksamkeit der Maßnahmen
  - Sicherheit bei Einkauf, Entwicklung und Wartung der IT-Systeme
  - Cyberhygiene (z.B. Updates) und Schulungen in Cybersicherheit
  - ....

- Erhebliche Sicherheitsvorfälle melden
  - innerhalb von 24 h ab Kenntnis Information an die Cybersicherheitsbehörde
  - innerhalb von drei Tagen ein ausführlicher Bericht
  - nach einem Monat ein Fortschritts-/Abschlussbericht

- Verantwortung der Geschäftsführung
  - muss Umsetzung der Maßnahmen überwachen und haftet für Verstöße
  - muss an Schulungen teilnehmen

- Registrierungspflicht für Unternehmen bei der Cybersicherheitsbehörde

NIS2UmsuCG –
NIS2 Umsetzungs- und Cybersicherheitsstärkungs-Gesetz

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital·Sicher·BSI·

NIS2UmsuCG –
NIS2 Umsetzungs- und Cybersicherheitsstärkungs-Gesetz
Hilfestellungen des BSI

Betroffenheitsprüfung auf Basis der EU-RL

FAQ

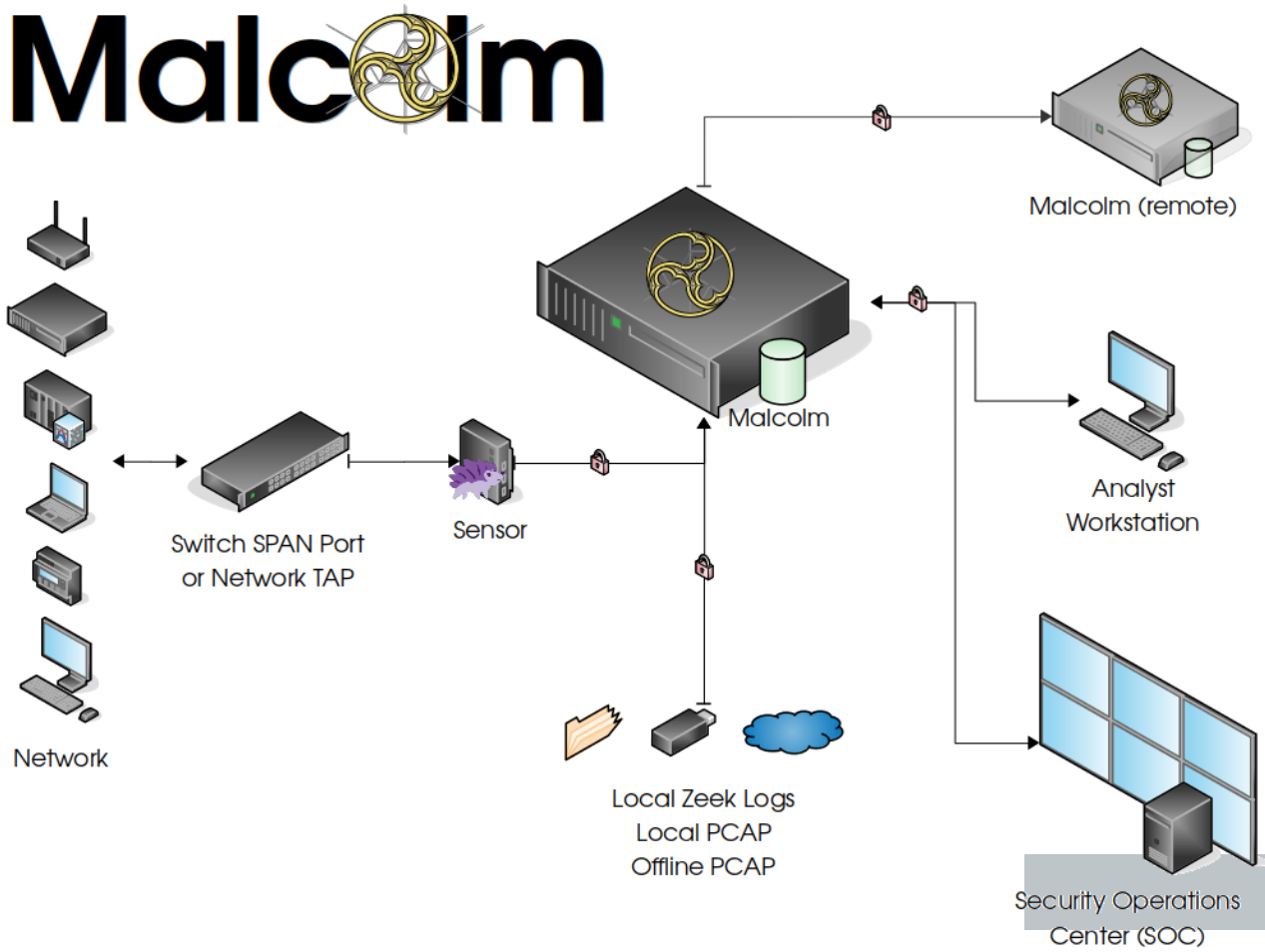
Was können Sie jetzt schon tun?

BSI IT-Grundschutz

- INF – Infrastruktur
  - INF.13 Technisches Gebäudemanagement
  - INF.14 Gebäudeautomation
- IND – Industrielle IT (Auswahl)
  - IND.1 Prozessleit- und Automatisierungstechnik (ISMS für OT)
  - IND.2 ICS-Komponenten
    - IND.2.1 Allgemeine ICS-Komponente
    - IND.2.3 Sensoren und Aktoren
  - IND.3.2 Fernwartung im industriellen Umfeld

MALCOLM - Netzwerkanalysetoolkit

- Open-source Netzwerkanalysetoolkit
  - Fokus auf ICS/SCADA Netzwerke (OT)
- Entwickelt bei Idaho National Laboratory (INL)
- Nutzung von bewährten Tools
  - Zeek
  - Suricata
  - Arkime
  - …
- Passive Netzwerkanalyse



https://github.com/cisagov/Malcolm

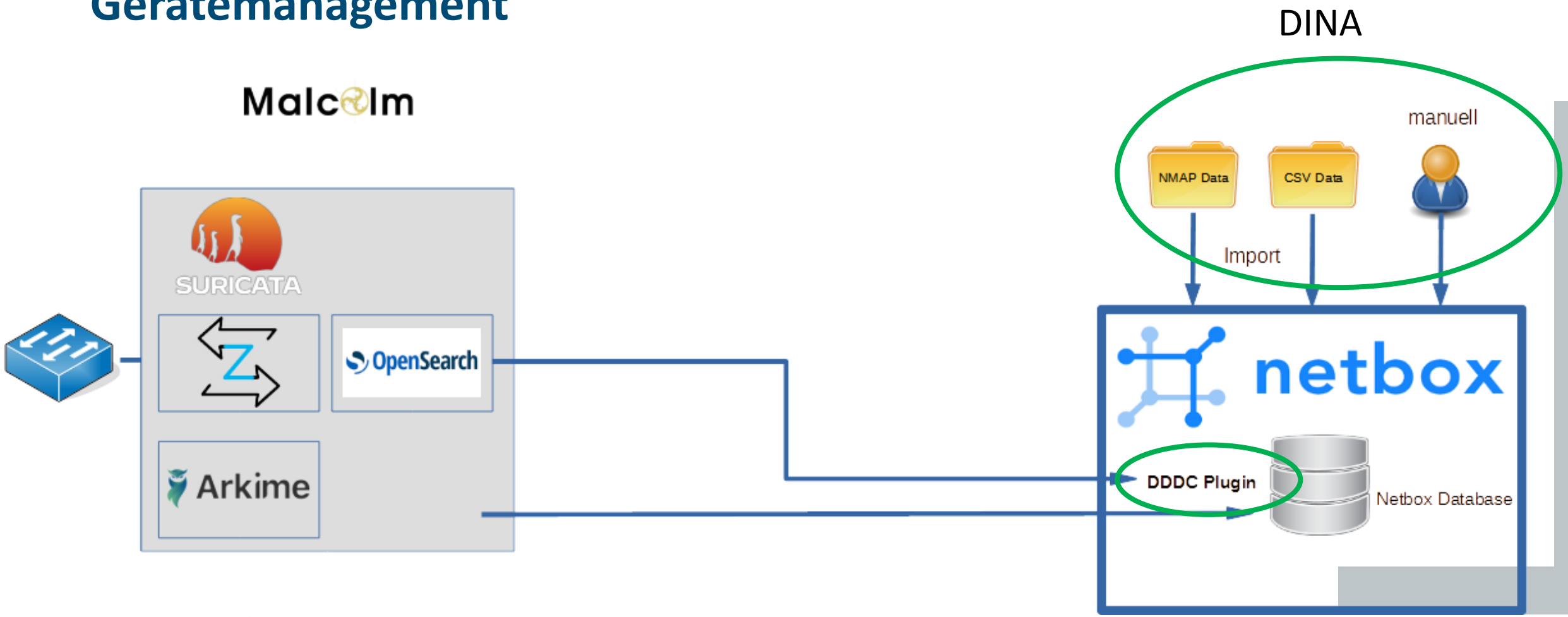
DINA - Detection and Identification of Network Assets

Weiterentwicklung der Open-Source Software MALCOLM

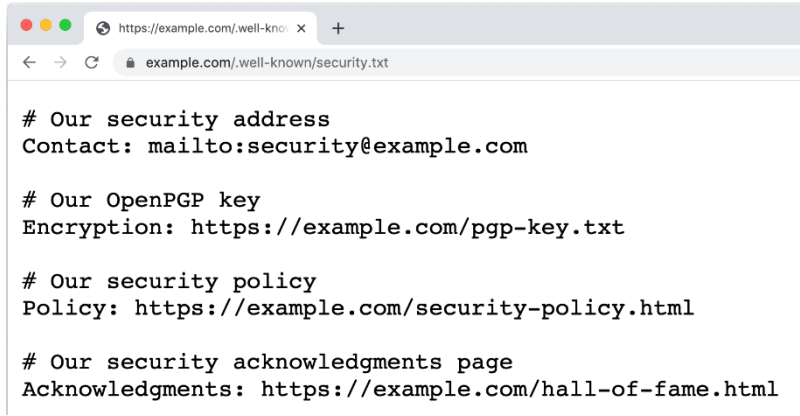
- Geräteidentifikation
- Geräteklassifikation
- Gerätemanagement
- Schwachstellemanagement (geplant)
- Open-Source Zeek-Dissektoren für fehlende Protokolltypen
- Aktive Geräteabfrage (angedacht)
- …

https://github.com/DINA-community

Gerätemanagement



Get started! RFC 9116 (aka security.txt) https://securitytxt.org



- Einfache Textdatei
- Standardisierter Ort

- Bekanntgabe einer Kontaktstelle für die Offenlegung von Schwachstellen;
  Unterstützt und gefördert durch:
  - CERTs: ACSC, BSI, CISA,…
  - Regierungen: Niederlande, Frankreich, Italien, Großbritannien,…
  - Firmen: Facebook, GitHub, Google, Cisco,…

https://findsecuritycontacts.com

CSAF – Die Eierlegendewollmilchsau?

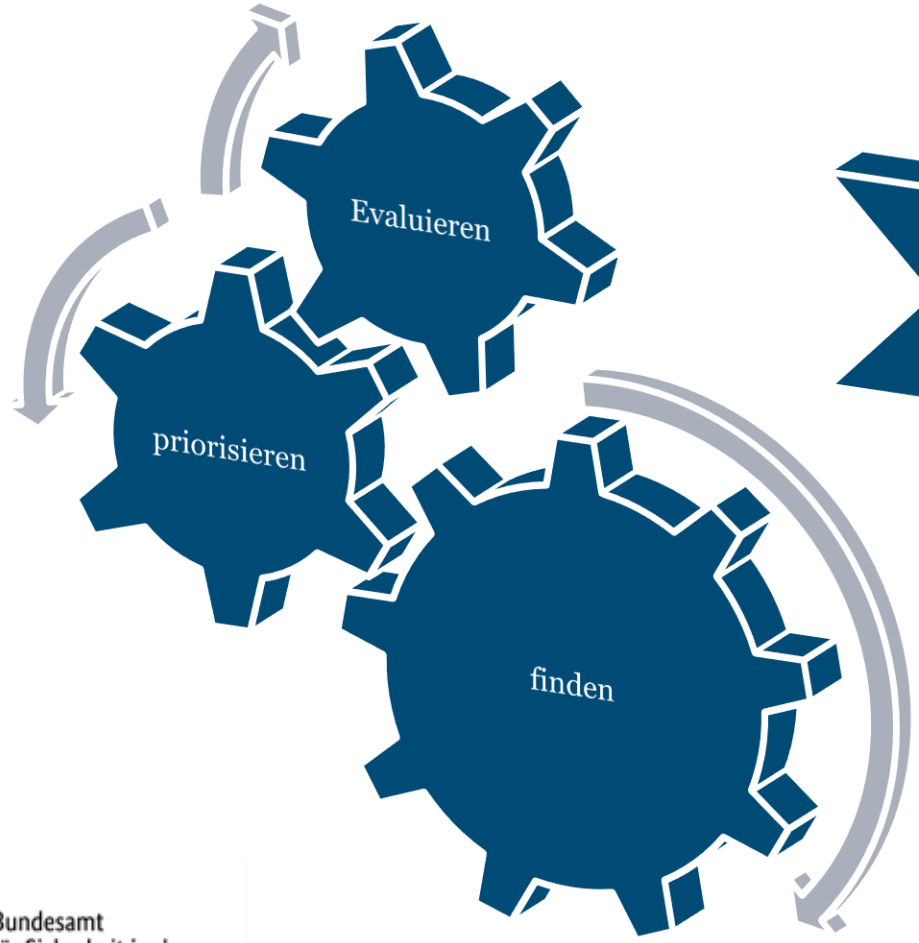
- Common Security Advisory Framework

https://www.kspch.ch

- Maschinenlesbares Format für Security Advisories (JSON)
- Open Source (OS) und OS Tools verfügbar
- Standardisiertes Format und standardisierte Weitergabe von Informationen
- Automatisierbarer Abruf und Vergleich (Asset Management)

Ready to use!

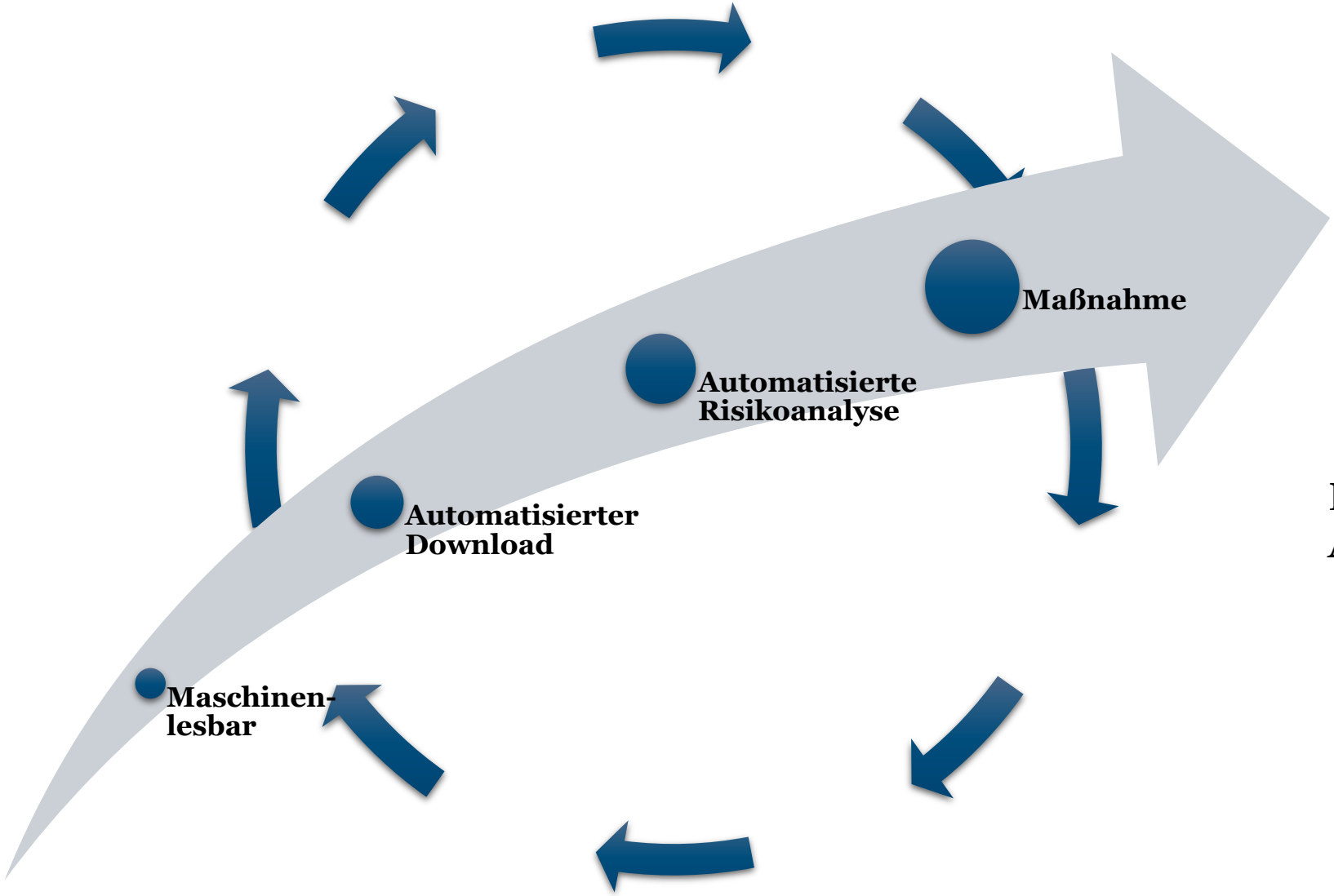
Manueller Prozess – the same procedure as with every Advisory…



Kritikalität des Advisories

- low
- medium
- high
- critical

Prozess mit CSAF – let‘s automate it!



Kritikalität des Advisories

- low
- medium
- high
- critical

CSAF – eine Revolution im Vulnerability Management

- Die Anzahl der Schwachstellen (CVE IDs) steigt stetig
- Es werden mehr und mehr Advisories veröffentlicht
- Advisories werden für die Risikoanalyse benötigt
- Automatisierung ist möglich
- Ein Format für alle und alles

https://cutewallpaper.org modified

→ **Please participate!**

Nebenbei bemerkt:
Unser Referat sucht Verstärkung!

Stellenausschreibung C25:

https://www.service.bund.de/IMPORTE/Stellenangebote/editor/BVA-BSI/2024/08/5667698.html

Bewerbung bis 25.09.2024!

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Jens Kluge
Referat Industrielle Steuerungs- und Automatisierungssysteme

ics-sec@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de/ics