Federal Office for Migration and Refugees

eu-LISA

Looking Ahead. Ensuring Cyber-resilience of EU IT Systems against Emerging Threats

Session III. Technology solutions for the IDENTIFY and PROTECT functions of the cybersecurity framework

From React to Act

Division 2: Digital Technologies, CIO, Innovation Management

The Federal Office for Migration and Refugees (BAMF) in Germany






Some facts:

- 8,300 employees in over 60 departments
  - 900 internal and external IT employees support approx. 150 IT products
- 244,132 asylum applications were received by the federal office in 2022
- > 3.4 million applications for asylum in the last 10 years, of which > 1.4 million in 2015 - 17

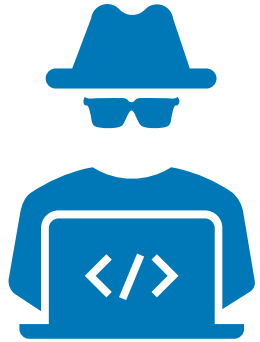
The Federal Office for Migration and Refugees (BAMF) is the centre of competence for asylum, migration and integration in Germany.

Today, it has a wide range of responsibilities:

- Implementation of the asylum procedure and decisions on asylum applications
- Promotion and coordination of integration
- Cooperation with security authorities
- International cooperation
- Research Centre for Migration, Integration and Asylum
- Digitalisation

Federal Office for Migration and Refugees

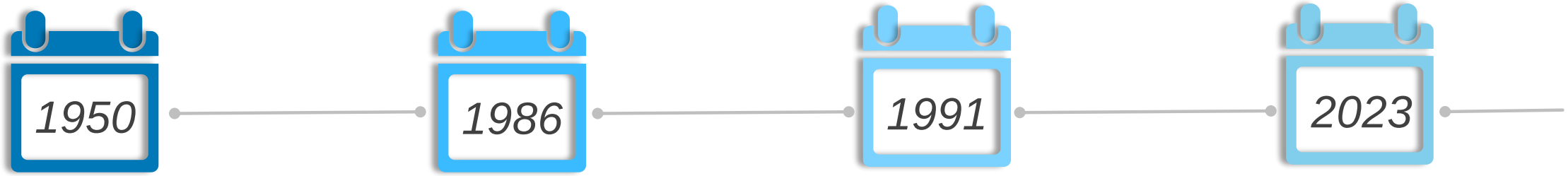
Journey - from react to act



Stay ahead of cybercriminals and be prepared to mitigate and counter emerging threats!

Federal Office for Migration and Refugees

Cybersecurity in Germany – a brief overview



- *Zentralstelle für das Chiffrierwesen (ZfCh)* was founded
- Central department for encryption/ciphering
- Office branch of *Bundesnachrichtendienst (BND)* - German Intelligence Service

- Working group within *ZfCh* began to work on questions regarding security due to rapid development within the IT-domain

- *Bundesamt für Sicherheit in der Informationstechnik (BSI)* was founded
- Federal Office for Information Security
- Independent from BND with focus on information security

- Federal offices which cover certain security aspects (BSI, ZITis, Cyberagentur, …)
- Individual federal offices from different federal department areas (environment, traffic, energy, ...) have their own cybersecurity departments

Federal Office for Migration and Refugees

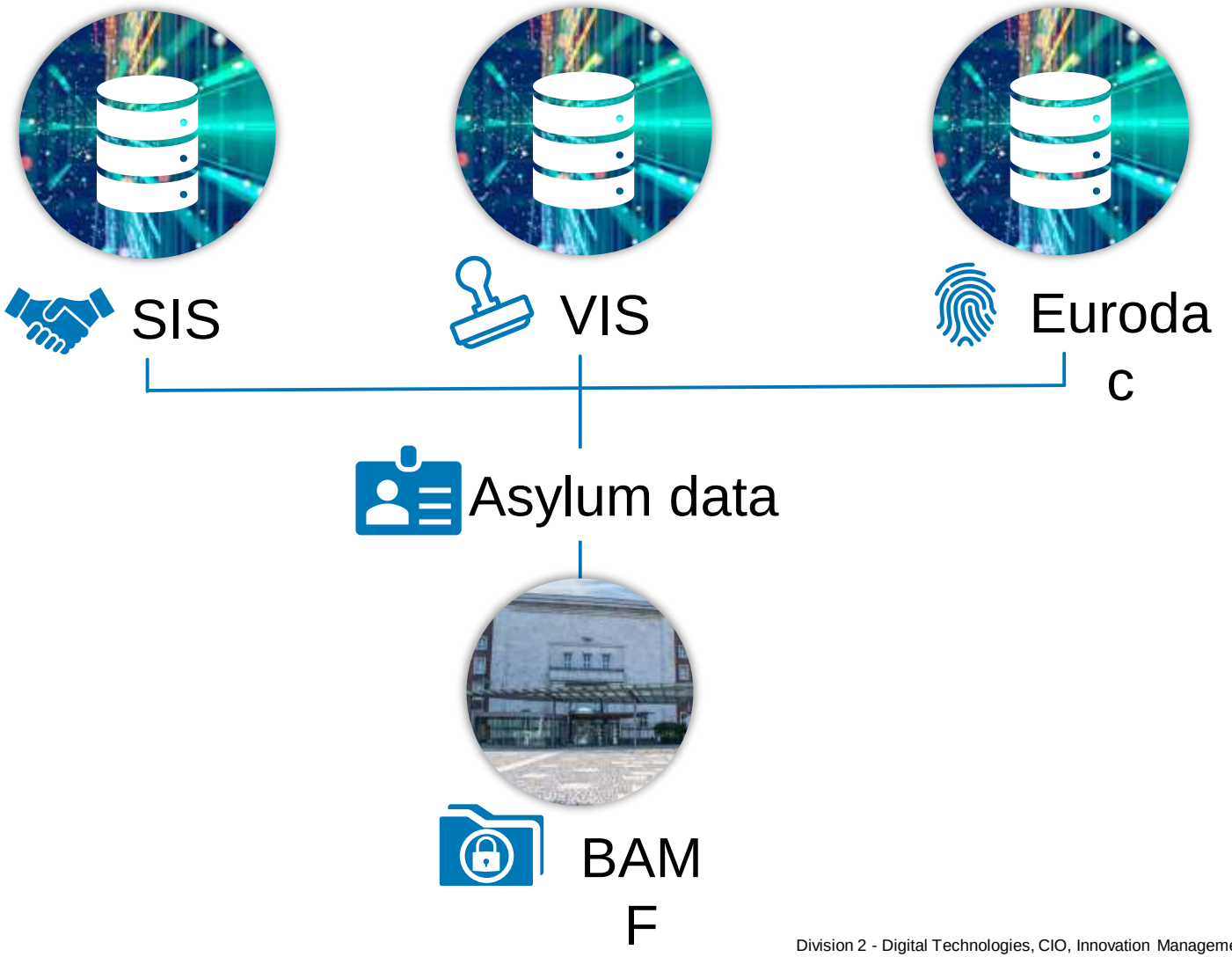
Cybersecurity Architecture of Germany

Source: https://www.stiftung-nv.de/en/publication/germanys-cybersecurity-architecture – 9th Edition, Stiftung Neue Verantwortung, CC-BY-SA 4.0

Link to Webpage from Stiftung Neue Verantwortung with interactive map of adjacent visualization. Also there is a descriptive publication available.

Federal Office for Migration and Refugees

Asylum data exchange between EU and Germany



Federal Office for Migration and Refugees

Cybersecurity @BAMF – A Journey

2005

- BAMF started to offer web services for seamless integration of processes and data transfer
- At that time, it was hard to protect webservices made available to external consumers
- BAMF had to craft own concepts to solve this by building solutions, which were developed later within the international web community

2006

We had to establish:

- Secure Gateway (name nor product did not even exist)
- Strong Authentication with SAML and later oAuth2
- Federated Identity Management with delegated administration of identities

2014

- BAMF had to face its biggest challenge
- Between 2014-2016 about one million Refugees came to Germany
- Huge impact on organization and IT-systems
- Workload growth up to 270%
- Scale vertically (servers, storage, network)
- Service-platform
  - Data-Service-Platform
- Mobile Registration
  - Distributed mobile stations for registration purposes
  - Developed within 4 months to manage the huge workload

2018

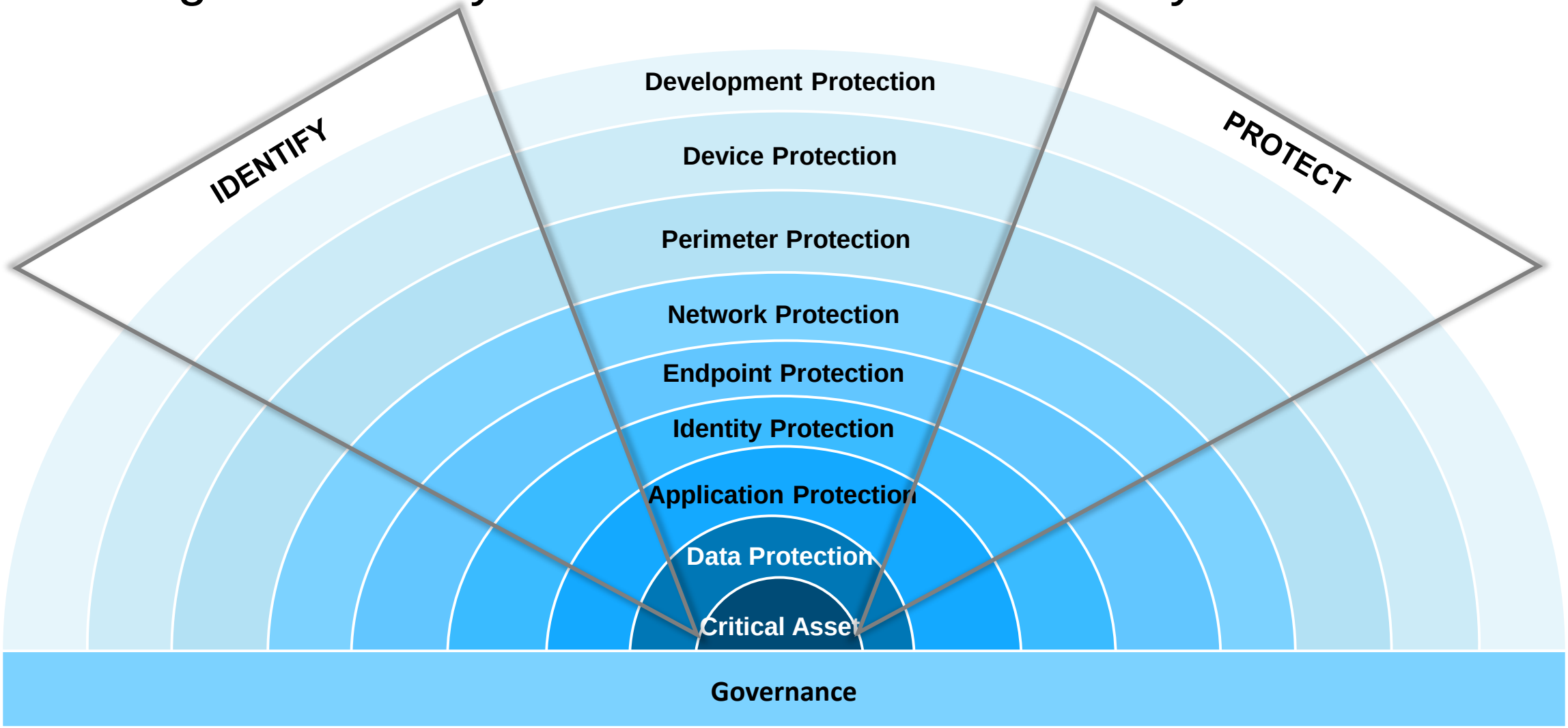
- BAMF developed a Vision which yielded in strategic projects
- Digital transformation was started to build a modern, flexible and agile agency
- Cloud-based / Cloud Native architecture
- Microservice oriented continuous deployment
- Develop and establish security framework for digital trust
  - Secure sensitive assets

Today

- Prospects
  - Recent enactment of European NIS-2 policy (January 2023) produces significant effort for BAMF
    - We are considered critical infrastructure now
    - Many other agencies face this issue
    - e.g. communal municipality management of Munich
  - BAMF needs to act accordingly to stay on top of the wave
  - Continuous process to build secure, reliable, and future-oriented organizational and technical systems
  - Focus on recent development and research

Federal Office for Migration and Refugees

BAMF-Igloo-Security-Framework - with Onion Layers



Federal Office for Migration and Refugees

Technics and patterns to secure applications

Secure Coding

- Secure coding - practice of developing software in a way that guards against the accidental introduction of security vulnerabilities
- **Code Scanner** SAST Static Code Analysis, DAST Dynamic Code Analysis; especially Fuzzing
- **Memory Safe Programming languages** like Go, Rust -> non-safe ones cause between 60% and 70% of vulnerabilities

Token Exchange

- **Digital Transformation** led into service **mesh** and **cascaded calls**
- Ensure **E2E identity recognition**
- **On-Behalf-Of (OBO)** with Token exchange is a key for End2End context
- **OIDC is not designed** to support **service mesh** natively – requires RFC-8693
- Consider **SideCar** Pattern to protect endpoints in cross cutting concerns manner

Attribute based Access & SSI

- **Role based Access Control** (RBAC) is limited for MicroService architectures -> consider **Attribute-based access control** (ABAC)
- **Fine grain decision making** in the context of attributes are required
- **Self Sovereign Identity** (SSI) is a key to secure resources in usage of attribute
- Introduce a policy based engine with dynamic trusted attribute evaluation (OIDC4VP)

Secrets-Management

- Secrets are commonly used in configuration files and not protected from system administrators
- Separate secret management from property management
- Never expose Secrets to Repos -> Consider SLSA
- **Rolling secret renewal**
- Reveal digital profile exposure, & proactively uncover risks associated to data leaks, breaches

Separate Read and Write

- Understand that 90% of app access are read operations. Separate them to gain high available and fine grain access control
- **Read and Write separation**
- **Command-Query-Responsibility-Segregation (CQRS)**
- Endpoint Security with 1:1 Provider – Consumer
- BAMF introduced the DataGrid-Concept for OLTP to secure data access from various consumer services

Developer Environment Protection

Developer IDE

- Understand and **respect the the developers' individuality** and establish secure and modern development tools
- **IDE extension threats** – often not in focus and they are an easy way to infiltrate and spy
- Tight integration of scanning capabilities to ensure **Secure Coding with Code Scanners** SAST Static Code Analysis, DAST Dynamic Code Analysis; especially Fuzzing

Developer-Env

- **CloudNative development** 60% coding and 40% configuration.
- Attack vectors are increasing, which is why the configuration also needs to be tested from the first day onwards
- Help developers take **proactive actions** by prioritizing remediations and strengthening controls

OSS Code & Artefact management

- Recognize the external dependencies are manifold due to Open Source movement.
- **Containers** (e.g. Docker), **code form public repos** and other assets are often weakly secured. That can be ex-ploited by intruders -> 50 % are out-of-the box insecure
- Provide **Inhouse Artefact Proxy Repository**
- Scan CVE in depth – Container Images, Layers and
- Use highly secure build packs

SWLC – Deployment Strategy

- Change is the normal behavior and not the exception.
- **Continuous deployment-automation** reduces time to react
- **Rolling Upgrades** to aim for zero downtime
- Introduce **architecture-design principles** like **12Factors, Stateless, etc.**
- **GitOps** – Establish a single source of truth with versioning

Federal Office for Migration and Refugees

Conclusion

- You can't buy Security
- You can't reach an absolute secure state in an organization
- You can't build fully secure systems
- Security has to be seen as a *continuous process*

- The *information* is there, the *methods* are there, the *tools* are there; and most importantly: The *people* are there
- 5 Dimensions need to be combined in the right context:
  Information, Awareness, Organization, Process, and Technology

If we stop or slow down in keeping up with continuous developments, we will give up advance

act instead of react

Federal Office for Migration and Refugees

Thank you and see you later

Federal Office for Migration and Refugees


Thank you and
see you later