DNS4EU

Hazai eredmények és kihívások
Networkshop 2024, Eger
Rigó Ernő

Intro

- Piacvezető alternatív publikus DNS szolgáltatás
  - EU kezdeményezés
  - nemzetközi konzorcium
- Célja: névfeloldó létrehozása
  - biztonságos, független
  - az EU-s szabályozásoknak (pl. NIS2) megfelelő
  - biztonsági eseményfolyamokon (CTI) alapuló szűrés
- Infrastruktúra szolgáltató ügyfelek
  - telekommunikációs cégek
  - kormányzati intézmények
  - testreszabott szolgáltatás
  - opc: saját névfeloldó (resolver) üzemeltetése
- HUN-REN SZTAKI HBIT szerepe
  - szolgáltatás terjesztése
  - piacfelmérés, kompatibilitási pontok kiemelése
  - magas szintű kiberbiztonsági tervezés

Hazai helyzetkép

NIS2 (2022/2555 EU irányelv)

NIS2 (2022/2555 EU irányelv)

(100) Az internet funkcionalitásának és integritásának megőrzése, valamint a DNS biztonságának és rezilienciájának előmozdítása érdekében ösztönözni kell az érdekelt feleket, köztük az uniós magánszektorbeli szervezeteket, a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóit, különösen az internet-hozzáférési szolgáltatókat és az online keresőprogram-szolgáltatókat, hogy fogadjanak el stratégiát a DNS címfeloldás diverzifikálására. ***A tagállamoknak ösztönözniük kell továbbá egy nyilvános és biztonságos európai DNS-címfeloldási szolgáltatás kifejlesztését és használatát.***

Hazai Internet szűrés lehetőségei

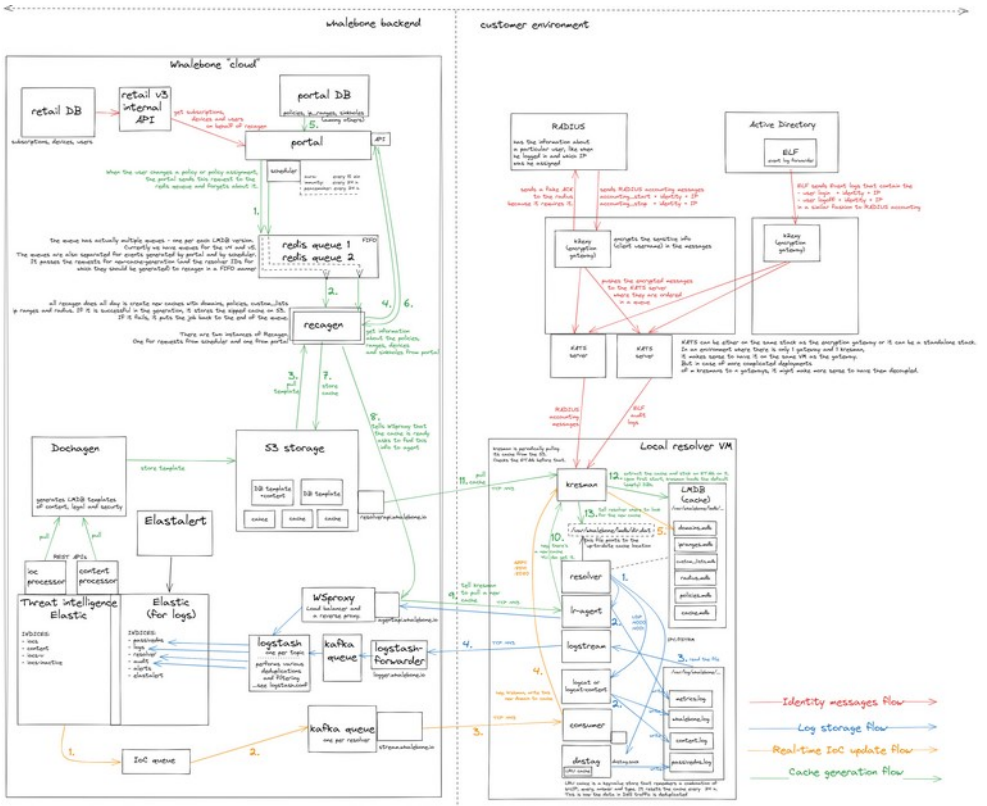
- Elektronikus adatok hozzáférhetetlenné tétele
  - NMHH hatáskör
    - EHT (2003. évi C. törvény) 92/A. §, 159/B.-159/C. §
  - központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisa (KEHTA)
  - hatósági vagy bírósági határozat alapján (írásos)
- Egyéb központi megoldás: nincs
- Jogszabályi környezet: bizonytalan
- Lehetséges szereplők
  - Nemzeti Média és Hírközlési Hatóság (NMHH)
  - Nemzeti Kibervédelmi Intézet (NKI)
  - Internet Szolgáltatók Tanácsa (ISZT)
  - Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ)
  - HUN-REN SZTAKI HBIT, HunCERT

DNS4EU

Biztonságtervezés

Architektúra

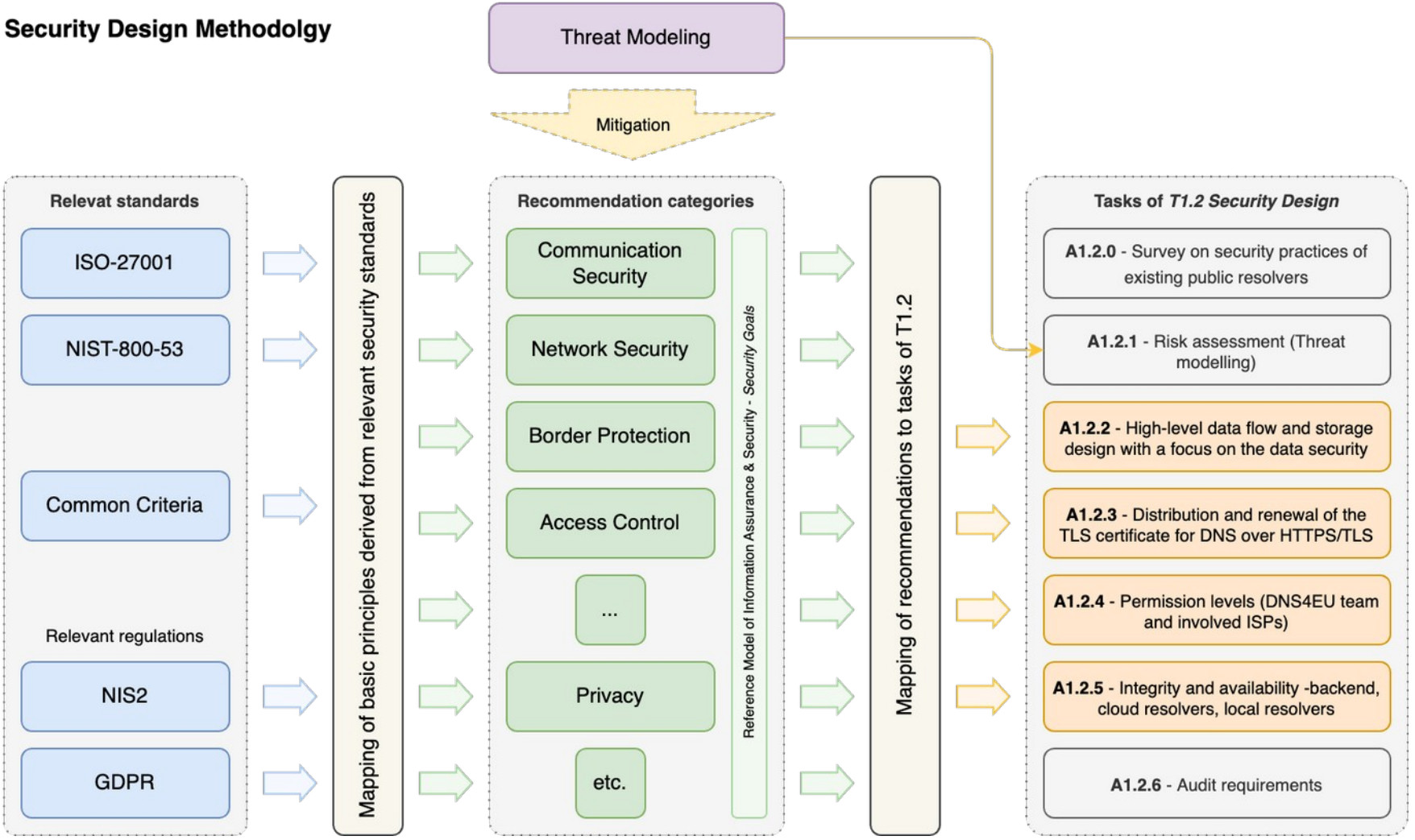
- Korszerű mikroszerviz alkalmazás (k8s)
- Összetett felhő backend
  - Elasticsearch (több példány)
  - S3 és egyéb tárolók
  - Ügyfélportál
  - Egyedi API végpontok
- Ügyféloldali deployment
  - Knot resolver
  - Batch és ondemand frissítési módok
- Mobil alkalmazás



Biztonsági architektúra tervezés

- Jelenleg létező publikus névfeloldó szolgáltatások biztonsági gyakorlatának vizsgálata
- Fenyegetettség modellezése
- Magas szintű adatáramlás, adattárolás megtervezése
- TLS tanúsítványok terjesztése és megújítása
- Hozzáférési szintek meghatározása a szolgáltatói körig bezárólag
- Sértetlenségre és elérhetőségre vonatkozó ajánlások
- Audit követelményeinek meghatározása

- Az eredménytermékek elkészítése és összefogása egyetlen biztonsági architektúrába:
  - Biztonsági célok és kategóriák meghatározása
  - Fenyegetettségek meghatározása és a kategorizálása
  - Kockázatcsökkentés módjának meghatározása a biztonsági kategóriák és fenyegetettségek közötti megfeleltetés létrehozásával
  - Biztonsági ajánlások megfogalmazása minden kategóriára (százas nagyságrendben)
- *A szoftver- illetve infrastruktúra biztonságra koncentrálva*

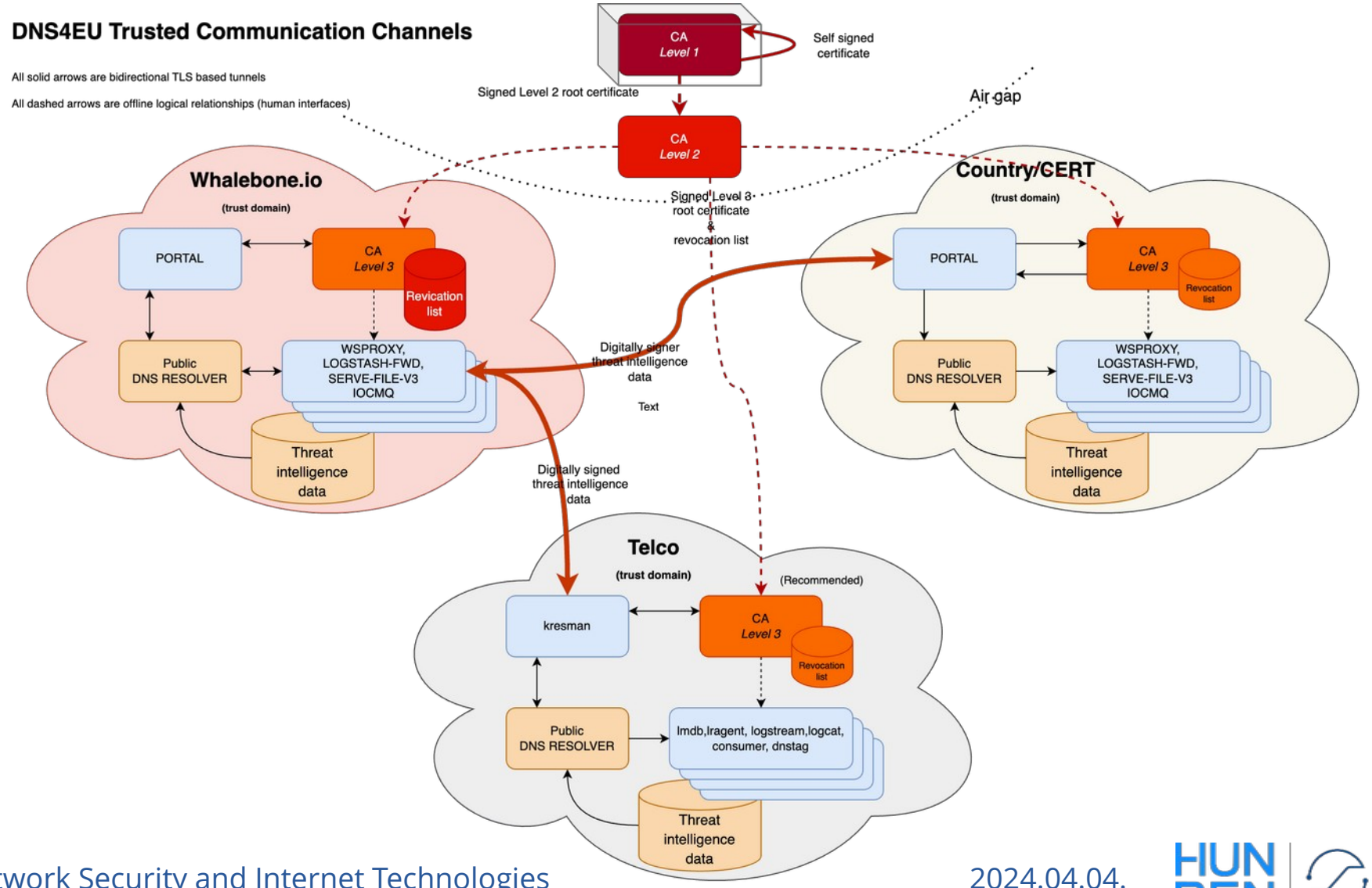

Security Design Methodolgy
Threat Modeling
Mitigation
Relevat standards
ISO-27001
NIST-800-53
Common Criteria
Relevant regulations
NIS2
GDPR
Mapping of basic principles derived from relevant security standards
Recommendation categories
Communication Security
Network Security
Border Protection
Access Control
...
Privacy
etc.
Reference Model of Information Assurance & Security - Security Goals
Mapping of recommendations to tasks of T1.2
Tasks of T1.2 Security Design
A1.2.0 - Survey on security practices of existing public resolvers
A1.2.1 - Risk assessment (Threat modelling)
A1.2.2 - High-level data flow and storage design with a focus on the data security
A1.2.3 - Distribution and renewal of the TLS certificate for DNS over HTTPS/TLS
A1.2.4 - Permission levels (DNS4EU team and involved ISPs)
A1.2.5 - Integrity and availability -backend, cloud resolvers, local resolvers
A1.2.6 - Audit requirements

Biztonsági modell

- Célok
  - Accountability
  - Auditability
  - Authenticity/ Trustworthiness
  - Availability
  - Confidentiality
  - Integrity
  - Non-repudiation
  - Privacy
- Fenyegetettségek
  - Third-Party Dependencies
  - System Weaknesses
  - Human Factor
  - Cloud-Specific Threats
  - Targeted Advanced Threats
  - Physical Security Threats
  - Regulatory and Compliance Threats
  - Emerging Threats
  - Disruption of Services

Biztonsági ajánlások

- Access Control
- Authentication
- Authorization
- Data Storage Integrity
- Communication & Cryptographic Support
- Privacy Related Measures
- Security Updates
- Perimeter Protection
- Network Segmentation
- Hardening
- Endpoint Security
- Input Validation
- Physical Security
- Security Management
- High Availability and Redundancy
- Backup and Recovery
- Log Management
- Security Event Management


DNS4EU Trusted Communication Channels
All solid arrows are bidirectional TLS based tunnels
All dashed arrows are offline logical relationships (human interfaces)
CA Level 1
Self signed certificate
Signed Level 2 root certificate
Air-gap
CA Level 2
Signed Level 3 root certificate & revocation list
Whalebone.io
(trust domain)
PORTAL
CA Level 3
Revication list
Public DNS RESOLVER
WSPROXY, LOGSTASH-FWD, SERVE-FILE-V3 IOCMQ
Threat intelligence data
Digitally signer threat intelligence data
Text
Country/CERT
(trust domain)
PORTAL
CA Level 3
Revocation list
Public DNS RESOLVER
WSPROXY, LOGSTASH-FWD, SERVE-FILE-V3 IOCMQ
Threat intelligence data
Digitally signed threat intelligence data
Telco
(trust domain)
(Recommended)
kresman
CA Level 3
Revocation list
Public DNS RESOLVER
lmdb,lragent, logstream,logcat, consumer, dnstag
Threat intelligence data

Köszönöm a figyelmet!

<rigo.erno@sztaki.hun-ren.hu>