Implementing Zero Trust at railways: Estonian example

Tõnu Tammer

CIO

Estonian Railways

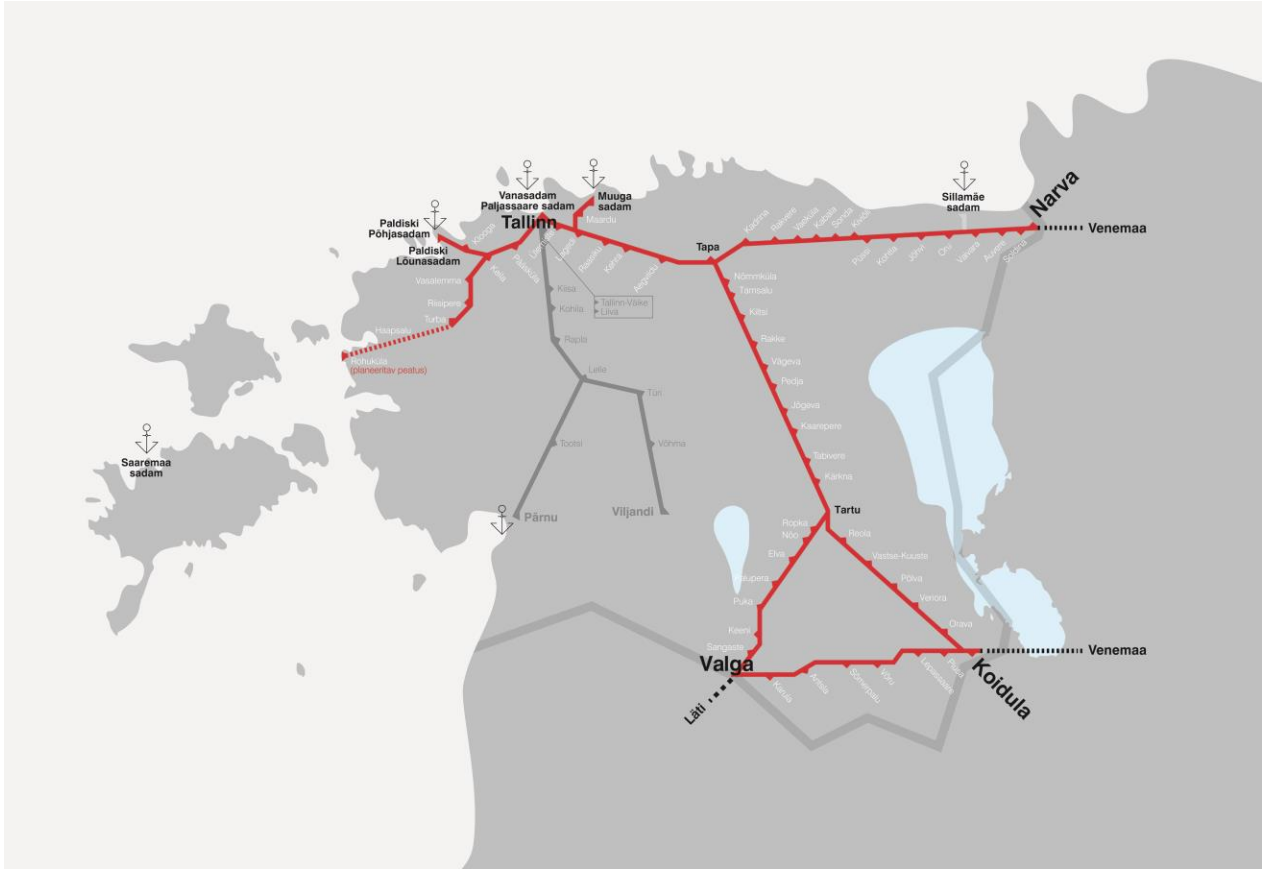
05.03.2025

Tõnu Tammer

- 15+ years in ICT / Cybersecurity
- 2022 → „100 most influencial people in Estonia“
- 2024 → awarded State Decoration: The Order of the White Star for „Promoting cybersecurity“
- CIO of Estonian Railways for over a year

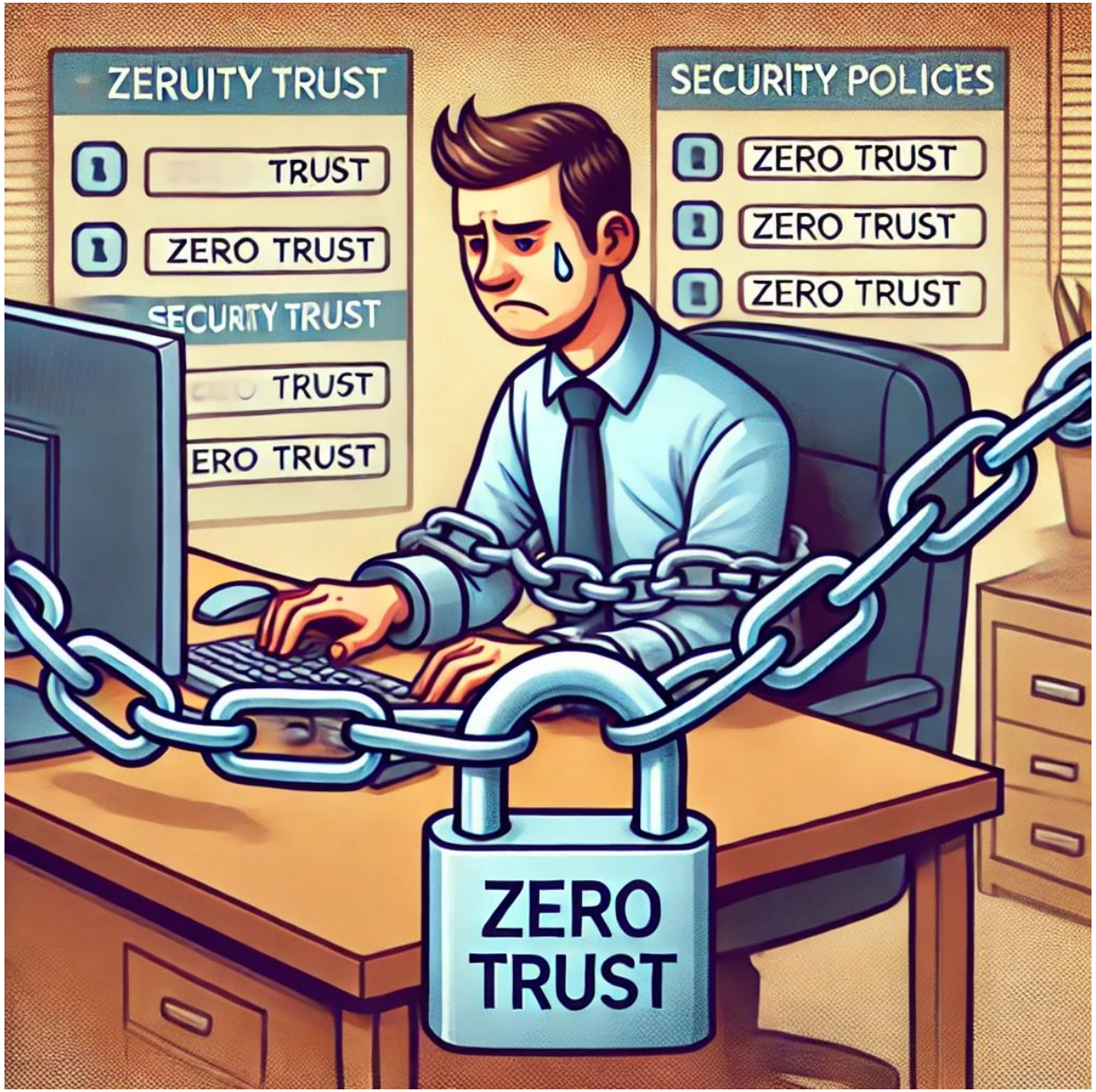
Estonian Railways

- Age: 154 years
- Length: over 1000km of tracks
- Employee: 17 years with company
- Employee: 50+ years of age
- Amount of legacy: plenty ☺



Principles of Zero Trust

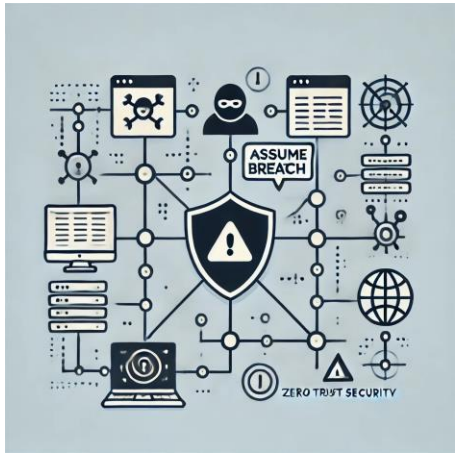
- The term "zero trust" was coined in April 1994 by Stephen Paul Marsh
- NIST defines zero trust as a set of cybersecurity paradigms:
  - move defenses from static, network-based perimeters to focus on users, assets, and resources.
  - It assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location.


ZERUITY TRUST
TRUST
ZERO TRUST
SECURITY TRUST
TRUST
ERO TRUST
SECURITY POLICES
ZERO TRUST
ZERO TRUST
ZERO TRUST
ZERO
TRUST

Raudselt koos
tulevikku!

Principles of Zero Trust

- Verify explicitly
- Least privilege access
- Assume breach



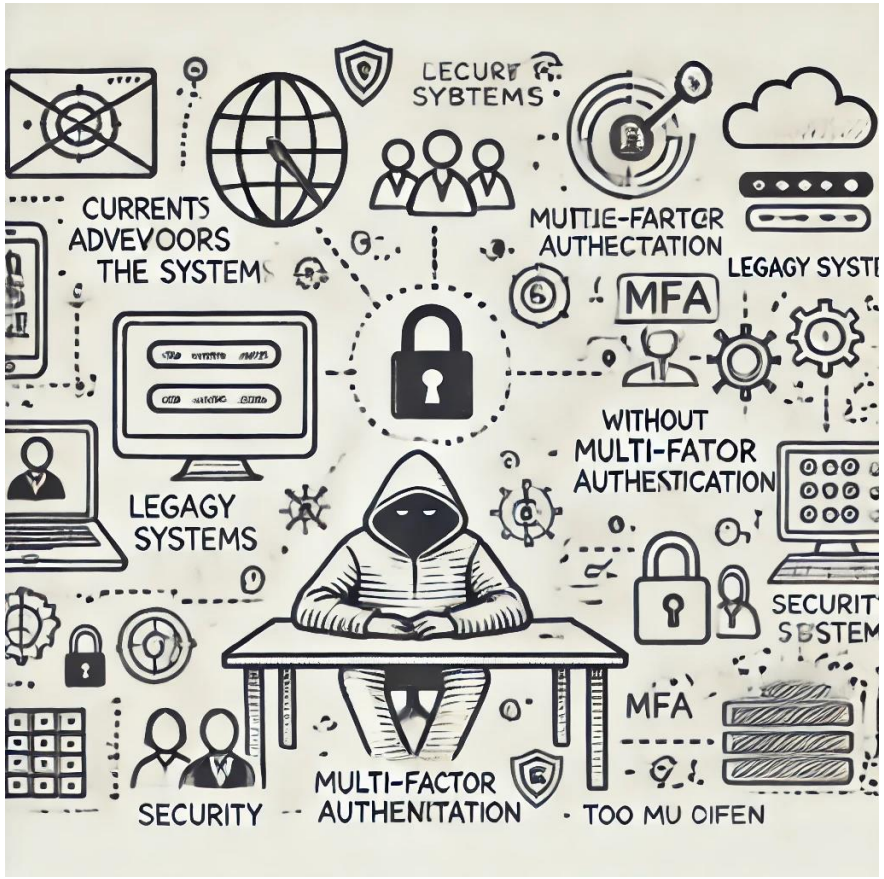
The reasons we had to make a change

Regulatory reasons

- GDPR – „… all appropriate technological protection and organisational measures have been implemented …“
  - Fines following a breach
- NIS2D requirements: added need to ensure business continuity
  - Fines before a breach

The reasons we had to make a change

- Current challenges
  - We are targeted by adversaries
  - Legacy systems
  - Users more out-of-office
  - Lack of multi-factor authentication
  - Too many different tech solutions



The reasons we had to make a change

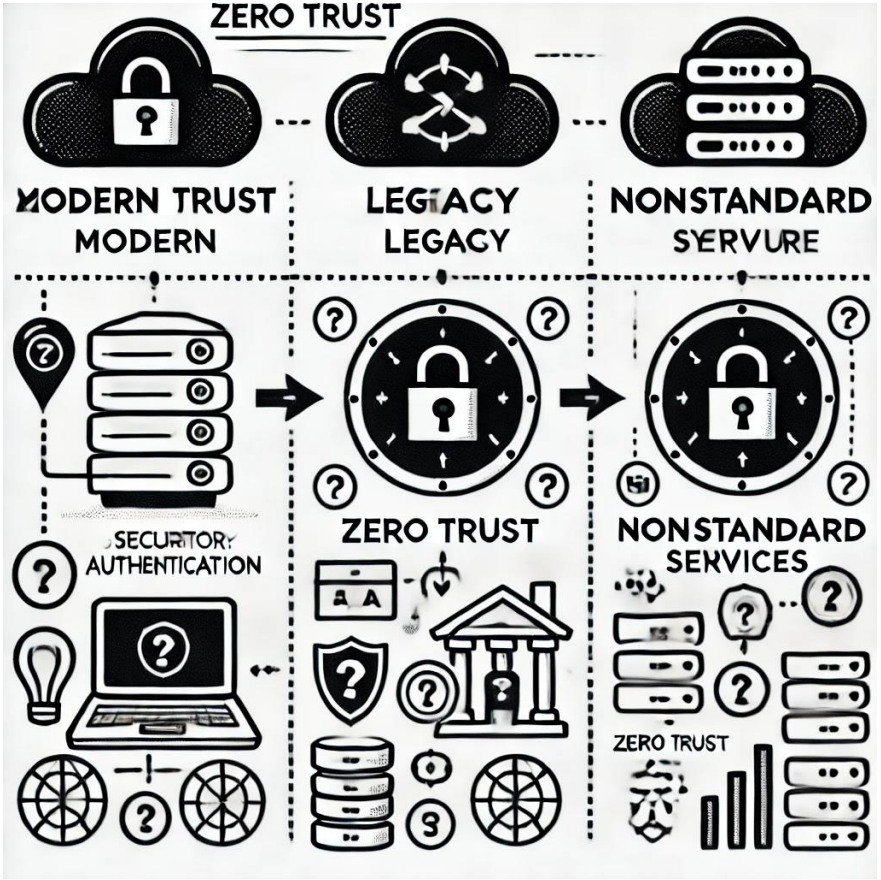
- Additional goals to achieve
  - The level of basic hygiene of end-users requires a technical solution
  - Need to have adequate resources for technology stack i.e., reduction of technical complexity
  - Do something with regards to external partners

Lessons in implementing Zero Trust

- Zero Trust – is nuanced

Lessons in implementing Zero Trust

- Many services
  - Modern
  - Legacy
  - Nonstandard services



Lessons in implementing Zero Trust

- Many users
  - Classic office use-cases
  - Field users
  - Different historical requirements

Lessons in implementing Zero Trust

- Many partners/services
  - Web services
  - SSH/RDP
  - Full WARP

Additional benefits for services!

- DDoS protection
- WAF
- CDN
- IPv6
- HTTP/3

Read more:
https://www.cloudflare.com/en-gb/case-studies/estonian-railways/

Thank you!
Question?

What did you patch today?

Tõnu Tammer

Tonu.Tammer@evr.ee