

# Dragons Watch – How to protect your assets? A practical perspective

APTLD86 - 09/2024 - Da Nang, Vietnam

Stefan Jakob

<jakob@denic.de>





# The InfoSec Team



# The actual InfoSec Team





# How do We deal with Risk and Security?

- Sadly, sometimes you can't, but you could raise the bar and be prepared to recover





# Security by Standards

- *Information Security Management System* (ISO 27001) since 2014
- *Certified Business Continuity Management Systems* (ISO 22301) since 2016
- Need to be compliant with German and European laws
- BSIG, KRITS, etc.
- EU directives **NIS2** and **RCE** define the EU framework for European critical infrastructure protection. Both NIS 2 (EU 2022/2555) and RCE (EU 2022/2557)





# We asked our colleagues

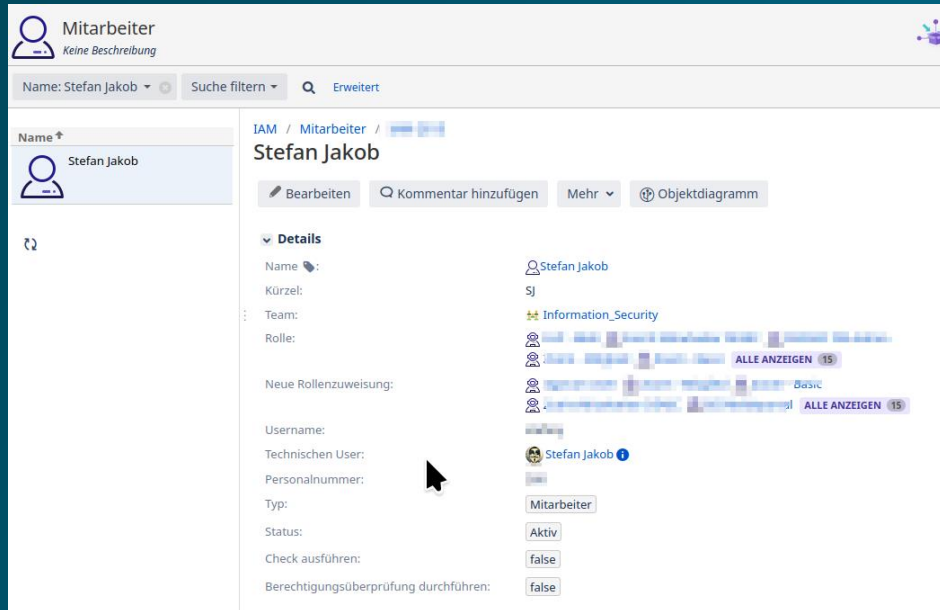
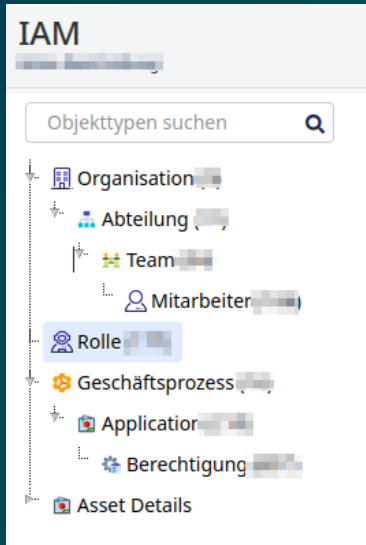
- What tools, rules, processes or measures do you think contribute to DENIC's security in practice?
- We got Feedback from 5 InfoSec colleagues  
12 people with good and strong technical background
- Sent statements as free text, but they should stand alone.
- *Aggregation by context and or content*
- Selected statements have at least 2 mentions
- Sorted by story plot



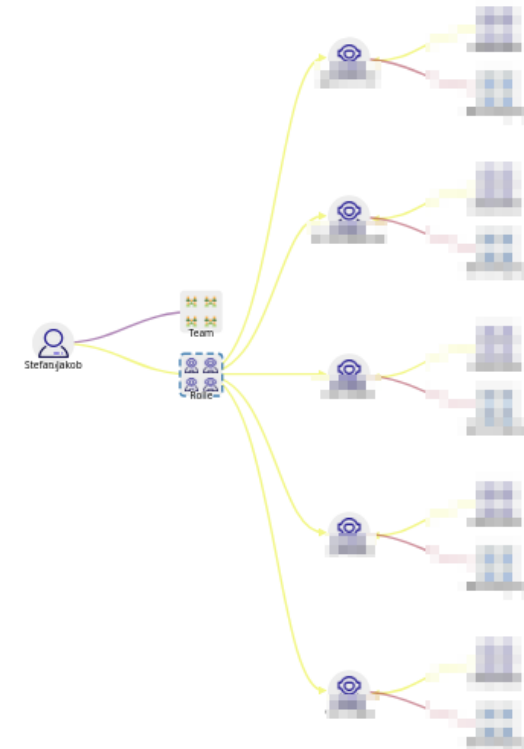
# Identity and Access Management (IAM)

- *IAM systems provide centralized control of permissions, prevent superuser rights, and simplify the onboarding process for new employees.*

# Identity and Access Management (IAM)



Objektdiagramm anzeigen





# Multi-Factor Authentication (2FA)

- *2FA is a proven method to secure access to critical systems and make attacks more difficult.*
- Always fly two errors high
- Access to VPN should be 2FA
- Services in the plain Internet should be 2FA enabled!

# Password Management

- *Using password managers and enforcing strict password policies enhances the security of access credentials.*
- Combine with 2FA/MFA to raise the bar
- Organisational structure, IAM and Password Management should show the same structure
- Use „vault“ systems to store passwords in you automation pipelines



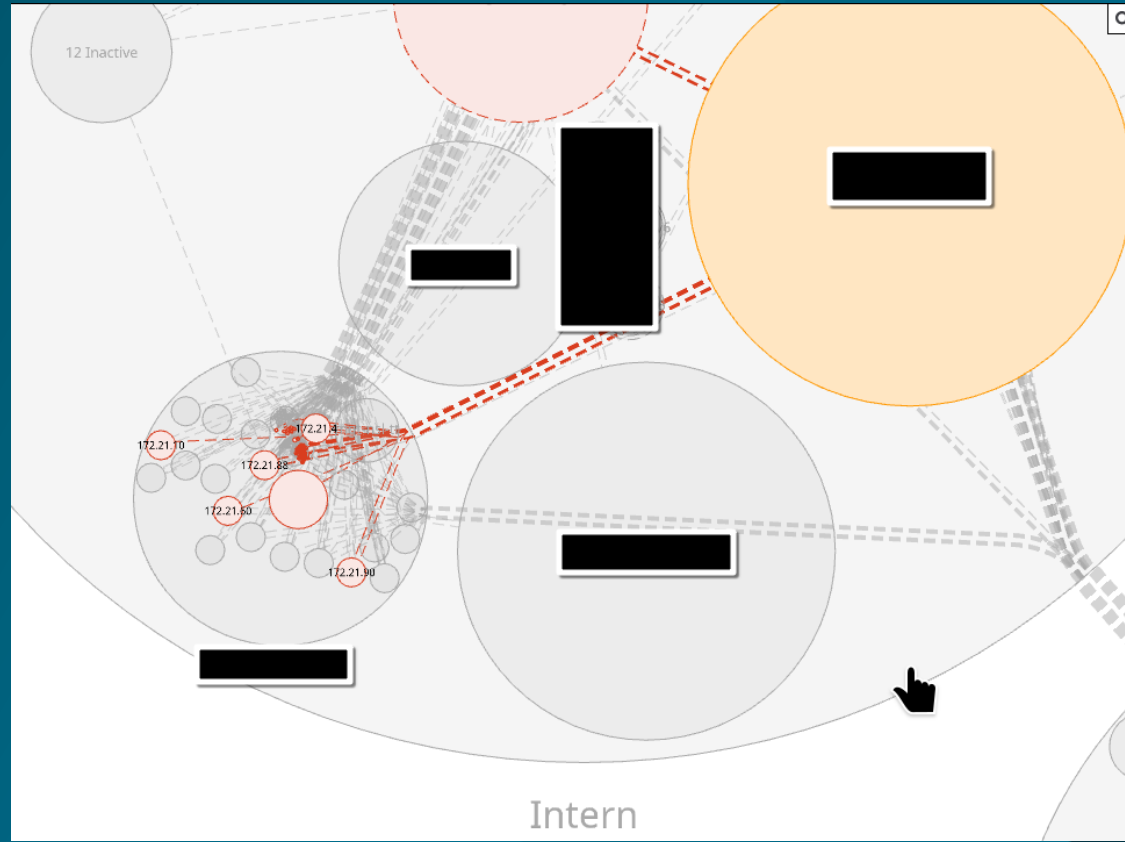
# Anomaly and Log Monitoring

- *By analyzing log data in tools like Elasticsearch/Kibana or through anomaly detection, security-relevant events can be identified early.*
- The definition of security use-cases helps teams to provide the necessary data. Avoid the haystack!
- Example: Do you see, count and alert „Failed Logins“ for all you systems?

alert.rev	4
alert.signature	DENIC Potential SSH Brute Force
alert.category	DENIC critical events
alert.severity	1
flow.pkts_toserver	13
flow.pkts_toclient	0

# Network Security and Monitoring

- *Firewall rules (default deny), Network Intrusion Detection, and comprehensive network segmentation ensure increased security.*
- IPAM, asset database and APIs to datasources are key for aggregated views!





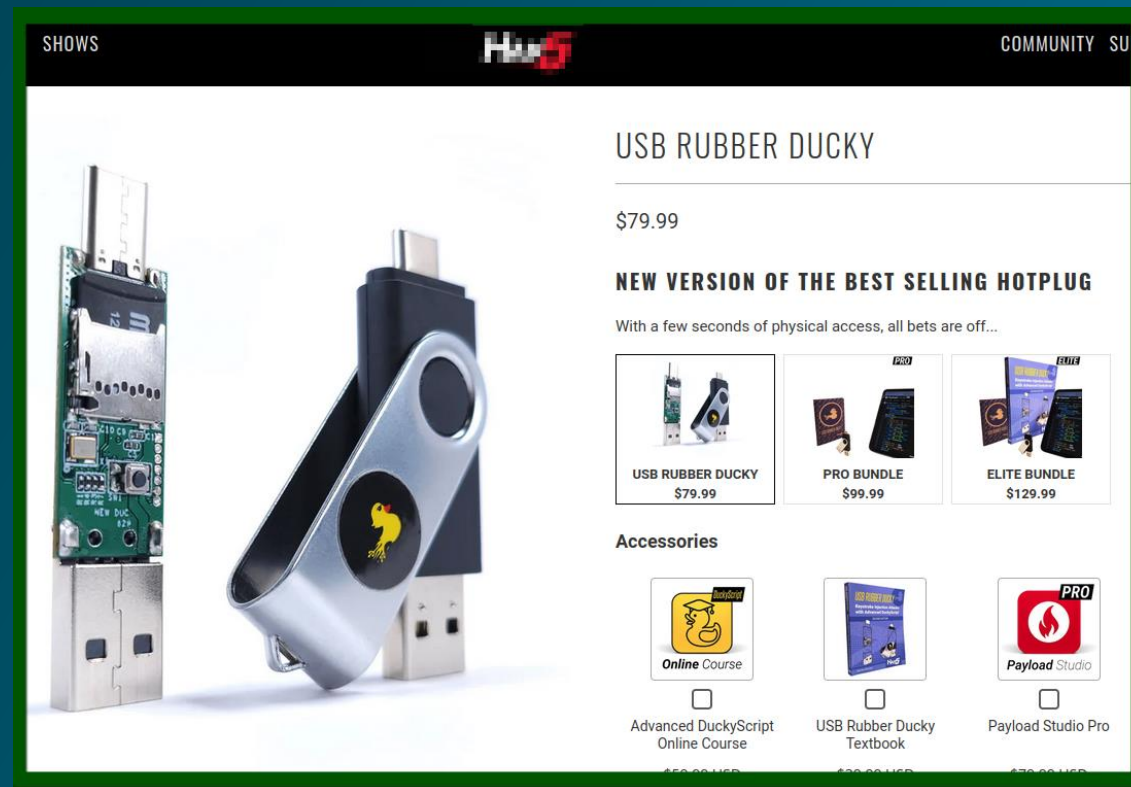
# Security Awareness and Training

- *Emergency exercises on a regular base*
- *Post-Mortems – Establish a culture of learning from incidents*
- Train realistic scenarios like
  - Malware on a colleagues device
  - Inside Infrastructure
  - Failure of components or a datacenter site
- Challenge your colleagues with out of box thinking
- Offer „easy“ guides for scenarios like „Malware Detected“



# Endpoint Protection

- *Endpoint security through antivirus software, firewalls, USB protection, and centrally managed solutions minimize vulnerabilities on devices.*



The screenshot shows the Hacking5 website's product page for the USB Rubber Ducky. The page features a large image of the device on the left, which is a silver USB drive with a black cap and a yellow duck logo. The right side of the page contains the following text and product listings:

**SHOWS** **Hacking5** **COMMUNITY** **SU**

## USB RUBBER DUCKY

\$79.99

**NEW VERSION OF THE BEST SELLING HOTPLUG**

With a few seconds of physical access, all bets are off...

Product	Price
USB RUBBER DUCKY	\$79.99
PRO BUNDLE	\$99.99
ELITE BUNDLE	\$129.99

**Accessories**

Product	Price
Advanced DuckyScript Online Course	\$59.99 USD
USB Rubber Ducky Textbook	\$39.99 USD
Payload Studio Pro	\$79.99 USD





# Backup Strategies

- *Strong backup solutions utilizing air gaps and WORM technologies provide comprehensive protection against data loss.*
- The time for a detecting a compromise is much longer as you would expect. 6M+ Does your retention match this?
- Data Escrow – Must have add-on
  - Securing Critical Data
  - Reducing the Risk of Third-Party Dependencies
  - Secure fail-safe for Disaster Recovery
  - Protection against internal and external attacks
  - Protection of intellectual property





# Redundancy and Diversity

- *By using different platforms, vendors, and technologies, we limit the impact of vulnerabilities and malware that target specific systems.*
- Operating systems
- Infrastructure
- People and Know-how
- Failure is an option, even with high standards
  - > Usage of anycast secondary provider

# Q & A







**THANK YOU!**

