Secure your checkmk

and sleep well ...

Ralf Spenneberg
30. April 2019
Check_MK Conference
Ralf Spenneberg

- OpenSource Security GmbH
  - Partner of Mathias Kettner GmbH since 2013
Security

- **Confidentiality**
  - Encryption

- **Integrity**
  - Authentication
  - Authorization

- **Availability**
  - Backups
  - Housekeeping
Security

- Do **not** reduce the security of the monitored systems
- Sensitive Data must be protected!
- The monitoring must be protected
Check_MK Built-In Security

• Agent
  - Runs as root but does not accept any data over the network
  - Manual Installation on the target system
  - The admin manages the Agent
  - Agent Update Mechanism is critical
    • Hardening of the Update-Server required
Agent – Recommended Security

- **SNMP**
  - Views
  - ACLs
  - SNMPv3

- **Agent**
  - only_from
  - Embedded Encryption (1.4.0)

- **Demo**
Check_MK Built-In Security

- Sites
  - Administration done as site user
  - Password/Public Key login possible
  - Internal switch to SSHA256 for passwords (1.6)
  - All processes use the site user
    - Apache
    - CMC/Nagios
    - Etc
    - Only icmpsender/receiver use root
- Root access only required for
  - Creation, removal and renaming of the sites
  - Update of the OMD/Check_MK Edition
Sites – Recommended Security

- Enable HTTPS and Redirect HTTP
- Use LDAP/SSL for user integration
- Use Password Store for Plugin Passwords
- It is a store but no password safe
- Demo
SSL Connections to Other Systems

- Do **not** ignore SSL errors!
- Add CA certificates
  - OS
  - Check_MK
- **Demo**
Distributed Monitoring

- Livestatus via TCP
- No restrictions by default
- Livestatus does not support any authentication nor authorization
- Distributed WATO may use SSL/TLS
- Livestatus supports commands!
Livestatus SSL/TLS Connections

- New Feature in 1.6
- In CEE and CRE
- Uses stunnel
- Demo
Analyze Configuration

- Best Practices
  - omdadmin/omd
  - SSL
  - Encrypted Backup
  - etc.
Discussion