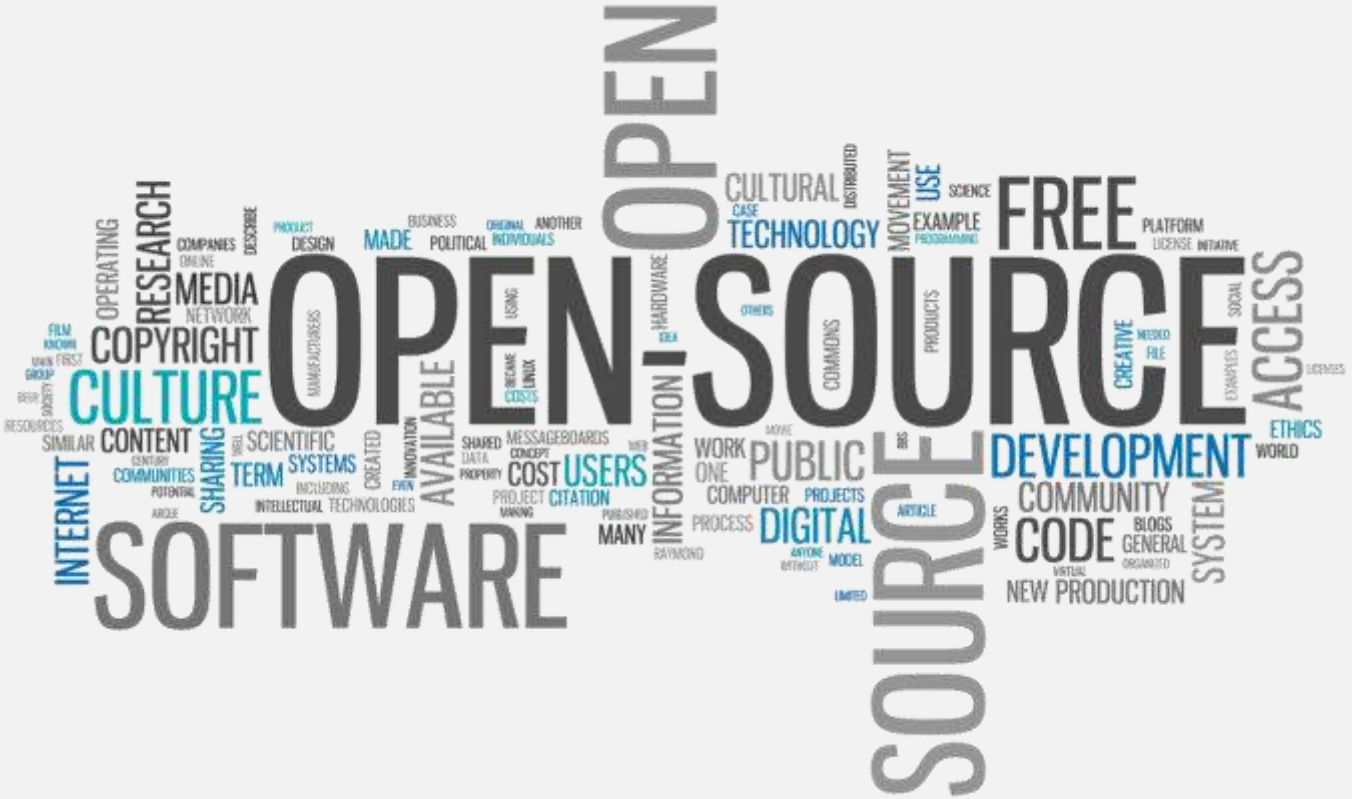

OSS as a pillar of EU NIS industry growth

Helmut Fallmann, Fabasoft

Introduction

- We see OSS as the most valuable source for new NIS tools as their sophistication increases and provides the basis for NIS tools and services.
- OSS offerings could form an essential basis for a future EU NIS industry.
- We have always contributed to OSS projects and see OSS NIS tools as more valuable than commercial NIS tools due to their transparency, tested effectiveness and breadth of contributors.

OSS for NIS

Encryption

OSS Tools – Today

- Transport encryption based on TLS
- Data-at-Rest encryption on filesystem level (EFS, SED)

OSS Tools – Demand

- End-2-End Data encryption on user devices with information sharing capabilities (beyond e-mail encryption)

Tool 1 of 6 >

OSS for NIS

Identity, authentication and access management

OSS Tools – Today

- OpenID, products for SAML or Shibboleth

OSS Tools – Demand

- Electronic identification and electronic Trust Services (eIDAS)

Tool 2 of 6 >

OSS for NIS

Endpoint protection (server, clients, mobile devices)

OSS Tools – Today

- Anti-virus
- Rootkit detection

OSS Tools – Demand

- Anti-malware, advanced threat protection

Tool 3 of 6 >

OSS for NIS

Firewalls

OSS Tools – Today

- Web application firewalls

OSS Tools – Demand

- Data center firewalls

Tool 4 of 6 >

OSS for NIS

Attack alert and identification tools (managed security services, SIEM systems)

OSS Tools – Today

- Network traffic analyzer
- Traffic monitoring tools
- Intrusion detection systems
- Packet sniffer, forensics

OSS Tools – Demand

- SIEM systems (Security information and event management)

Tool 5 of 6 >

OSS for NIS

Scanning and exploitation tools

OSS Tools – Today

- Packet crafting, packet sniffers
- Port scanners
- Vulnerability exploitation tools
- Vulnerability scanners

OSS Tools – Demand

- none

Tool 6 of 6

Documentation and Evidence

- Certifications require effective security related controls and evidence.
- We would like to see OSS tools supporting automatic documentation and evidence collection of controls performed.

Summary

- What we need is an OSS-based, not proprietary, set of NIS utilities (technical and management) with trustable secure capability. This also requires public standards for secure operations that the OSS NIS modules shall comply with.

Thank you for your attention

Copyright / Disclaimer

- Copyright © Fabasoft Austria GmbH, Linz, Austria, 2016.
- All rights reserved. All hardware and software names used are trade names and/or brand names of the respective manufacturer. Fabasoft accepts in this document no explicit or implicit responsibilities, in particular not as regards the completeness and correctness of the document. This presentation contains forward looking statements, including information using the words “believe”, “assume”, “expect” or formulations with a similar meaning. Such forward-looking statements comprise known and unknown risks, uncertainties and other factors, that can result in the fact that the real results, development, financial situation or achievements deviate considerably form those assumed implicitly or explicitly in those statements. These factors among other things include: competition through other companies, effects or risks of new software and technology, the company’s ongoing capital needs, financing costs, changes in the operating expenses, engaging and keeping of qualified employees, disadvantageous changes in the applicable fiscal law, riots, cause beyond control, acts of war and other in this presentation named factors. In connection with these uncertainties investors should not rely on those forward-looking statements. The company does not accept any responsibilities, to comply with those forward-looking statements in the future or to adjust them to future events or developments.
- Photo credit “open source graphic“: Shutterstock/mindscanner
- E&OE.