

Sicherheit durch Open Source ?!

Markus Hennig
CTO, Astaro

Open Source?



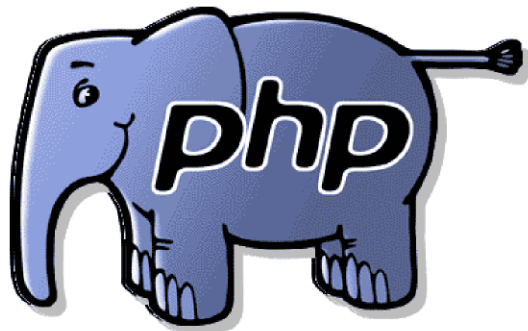
Open Source!



Open Source – the most famous



PostgreSQL







Linux Foundation 2008:

- 33.00 files
- 13Mill LoC
- 7500 Man Year
- 1.4 Mrd\$ value

Sicherheit durch Open Source?

- Why not?
- AES, 3DES \leftrightarrow WEP, DECT, GSM A5/1 A5/2
- Secrecy \leftrightarrow Security
- Security is not a state, but a process!
- Security is not absolute, but relative!
- Real security is not compromised when people become aware of it

Security Myths about Open Source

- ◆ Eyes that look do not always see
- ◆ High level of complexity in the code prevents most users from in-depth audit
- ◆ "Hotspots" in the code are reviewed regularly - others parts are not
- ◆ Large tester-base can not show the absence of bugs, therefore you need qualified code security examination
- ◆ You not only have friendly code analysts, there are also hostile ones
- ◆ Open source is no security panacea

Open Source in Astaro Produkten



Common Criteria
EAL 4+

The Netfilter project as an example



- Description: Linux packet filter, featuring stateful firewalling, all variations of NAT and load balancing – and packet mangling
- the project was founded in 1999 in Australia, currently has 5 core members and more than 700 contributors of significant code parts
- grew to 93.000 lines of code in 3 years, average of 1.400 postings/month on the devel mailing lists, currently around 300 active developers
- 65 code improvements or fixes/month per stable release from the community
- example: FTP-contrack bug being fixed during 'off hours' while Astaro developers were sleeping
- according to the questions asked on the mailing lists from different authors, Astaro believes thousands are examining the code

(Netfilter, 2003)

Astaro Company Profile

- **Founded 2000**
- **220 employees**
- **Headquarters in:**
 - Karlsruhe (Germany)
 - Boston (USA)
- **Worldwide Offices**
- **> 3000 partners & resellers worldwide**
- **24/7 Service**
- **Astaro protects more than 100.000 networks for ca. 60.000 customers in over 60 countries**



The Astaro Difference

- Only Astaro appliances are available in three different types

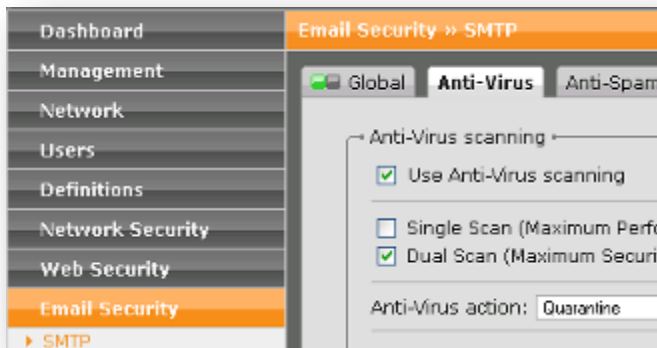


- Nobody's more flexible



One-Click Clustering

- Nobody's faster

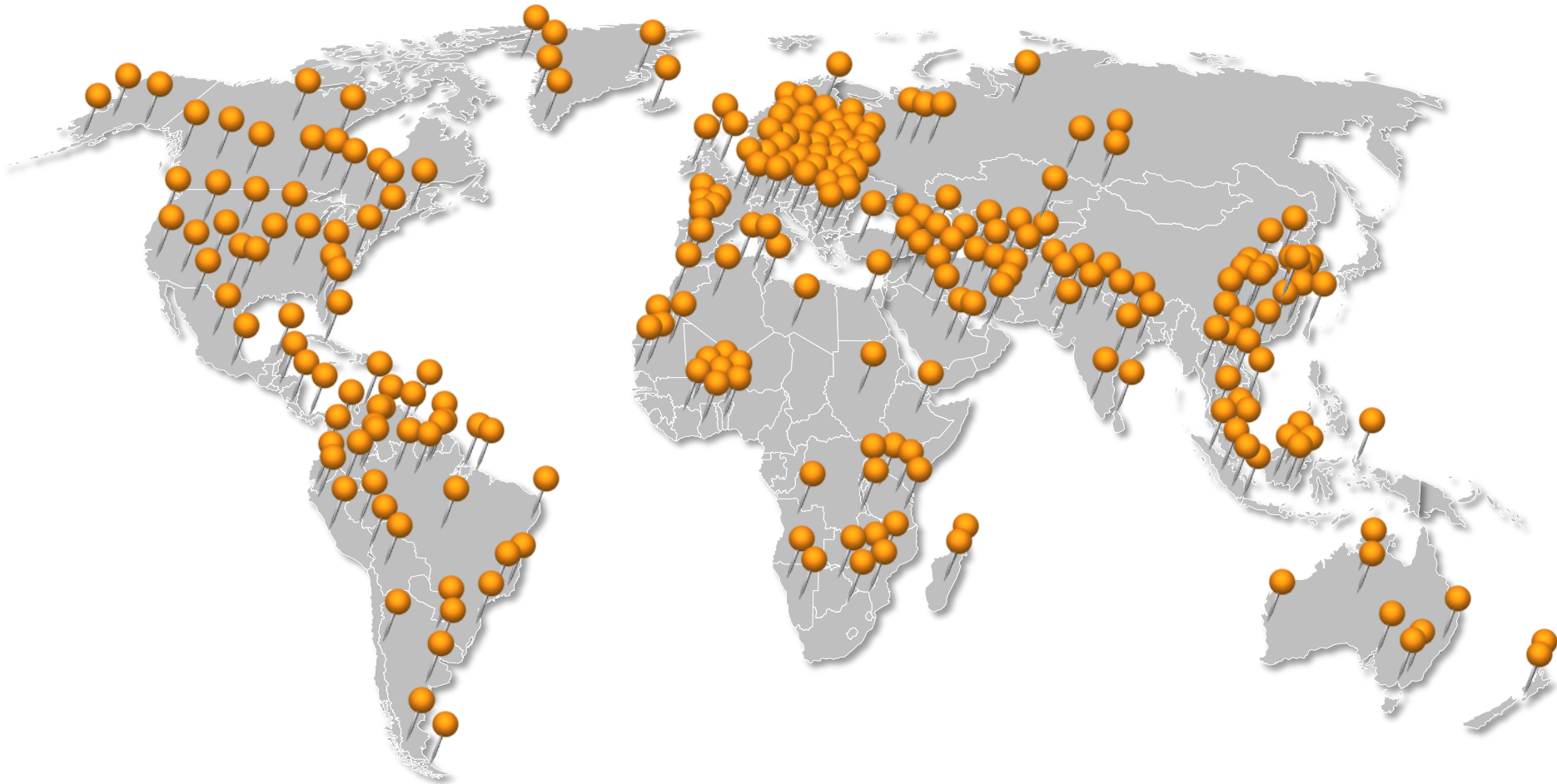


10-Minute-Setup

- Prooven technology

Over 60,000 customers are already protecting more than 100,000 networks with an Astaro appliance

Weltweites Netzwerk von zertifizierten Partnern



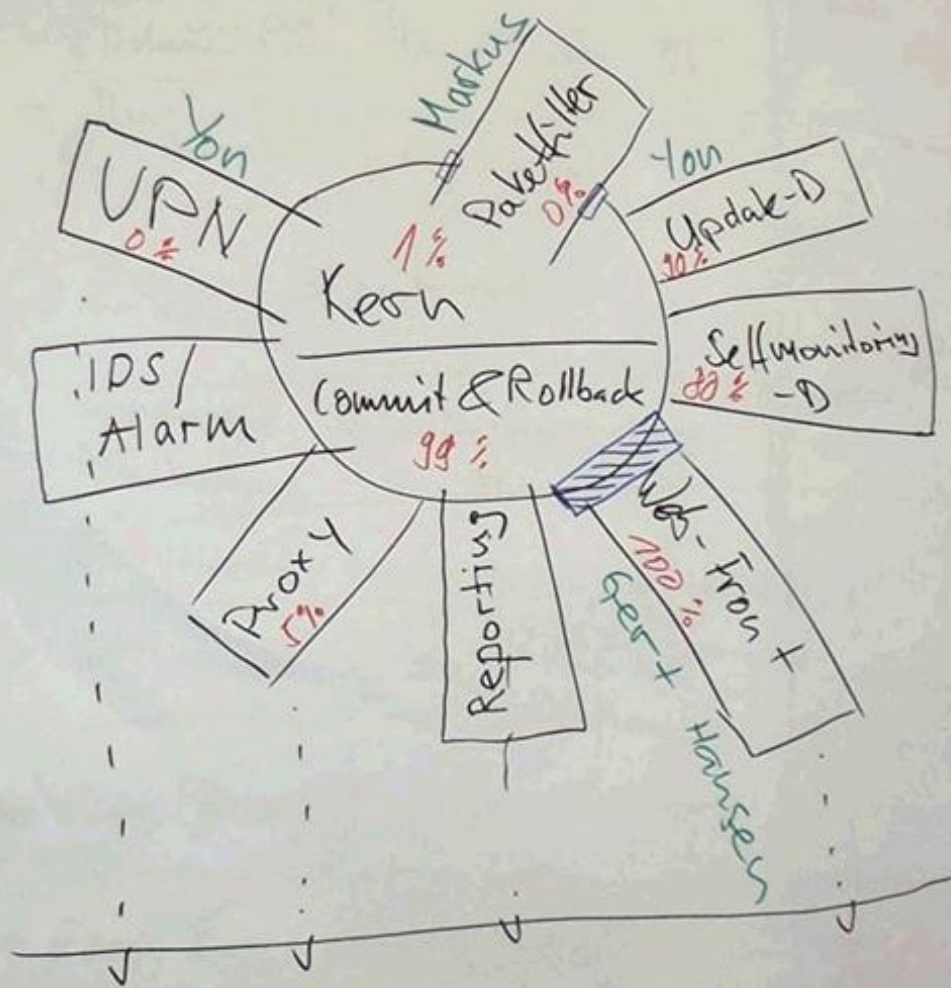
Astaro Unified Threat Management Appliances




Astaro 2000

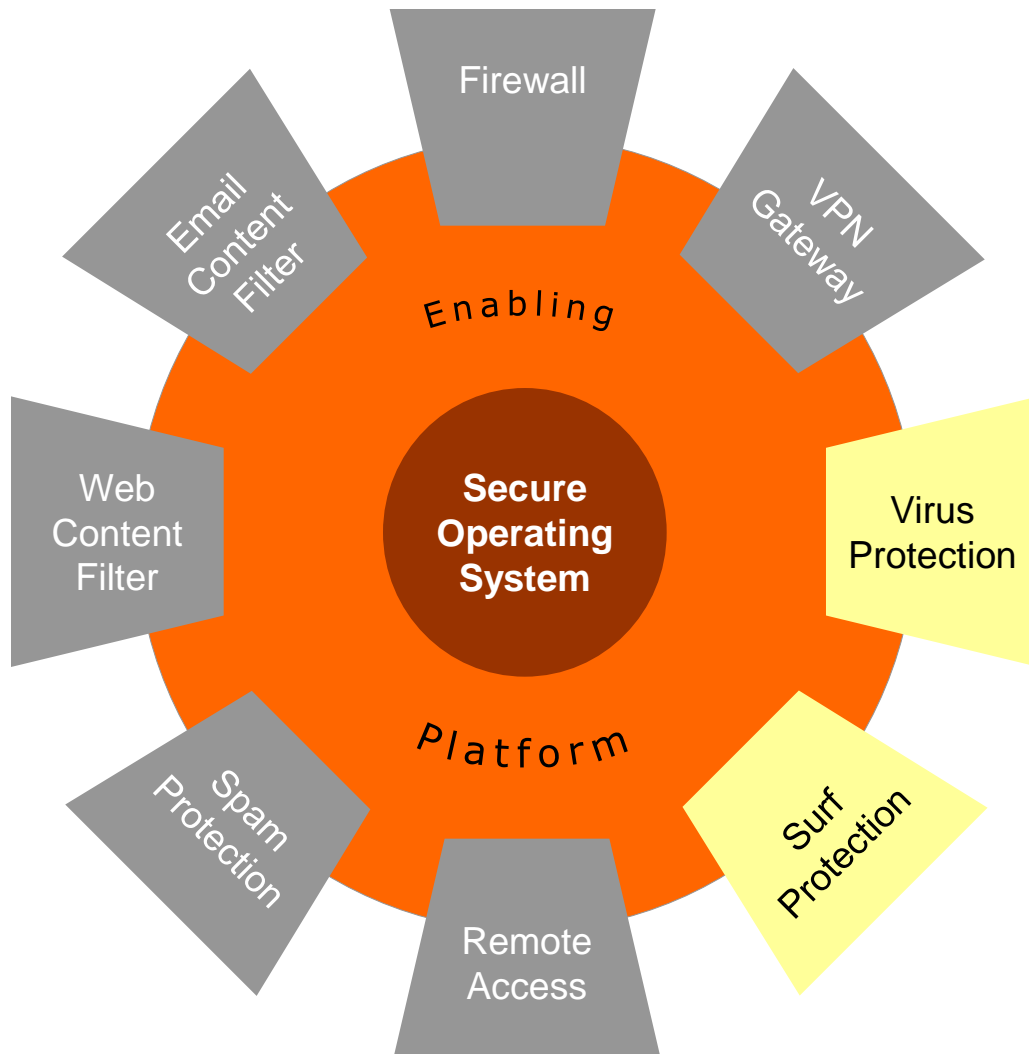


% - proportion



 - Doku-System

Astaro Security Gateway-Architecture



Astaro enhanced Linux

Hardened Linux Distribution with installation wizard and automatic hardware detection

Proprietary platform

The glue for easy-to-use products: MiddleWare, WebAdmin, Confid, Up2Date, SelfMonitor, High Availability

Open Source applications

Cutting-edge security applications like netfilter, squid, exim etc. Mostly first out there and very reliable.

Proprietary applications

Range of proprietary Astaro and 3rd party technologies for up-selling, currently virus scanner and URL list

- Open Source : used as a general term for software with source code open to read for “everybody”
- Different licenses usable: BSD, GPL, Artistic License, similar licenses models from SUN, Microsoft, ...

What is interesting on Open Source?

- ◆ Projects
- ◆ Programs
- ◆ Products
- ◆ Source Code
- ◆ Method
- ◆ Organization
- ◆ Involved people
- ◆ Involved Organization

Using Open Source

- Open Source ist Mittel zum Zweck, nicht Selbstzweck
- Open Source Code $\leftarrow \dots \rightarrow$ Organisation, Methode, Leute
- Open Source: Mozilla, KDE – Linux, OpenSSL – lighttpd, JsTetris

Using Open Source

- Open Source ist Mittel zum Zweck, nicht Selbstzweck
- Open Source Code ← ... → Organisation, Methode, Leute
- Open Source: Mozilla, KDE – Linux, OpenSSL – lighttpd, JsTetris

- Open Source ist auch eine Methode:
 - distributed, de-central, un-democratic
 - open and flexible
 - without costs
 - difference to “commercial” software engineering
- GPL: GNU Public License is a valid software license
- Kunden:
 - interessiert OS überhaupt nicht
 - wollen ein Produkt, kein OS Projekt
 - vergleichen TCO, nicht frei verfügbaren Source Code



Vielen Dank!
Fragen?