

dn

Germany

Systems

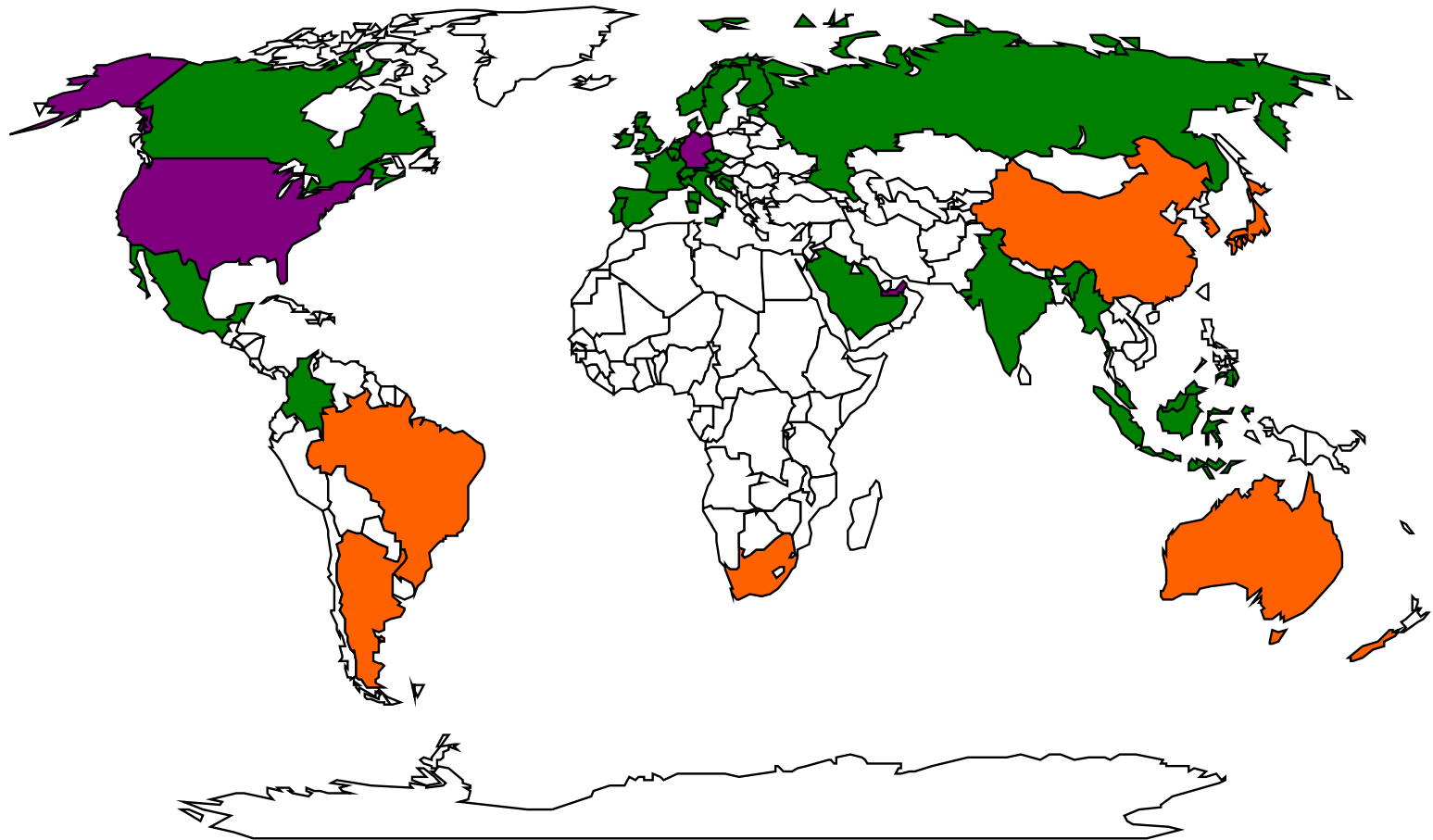
**What you should know
running your Linux box secure**

About DN-Systems

- Global consulting and technology company
 - Planing
 - Evaluation
 - Audit
 - Computer and network laboratory
 - Project management
 - Integral security (not only IT)
 - Investigation / digital forensics

Worldwide Service

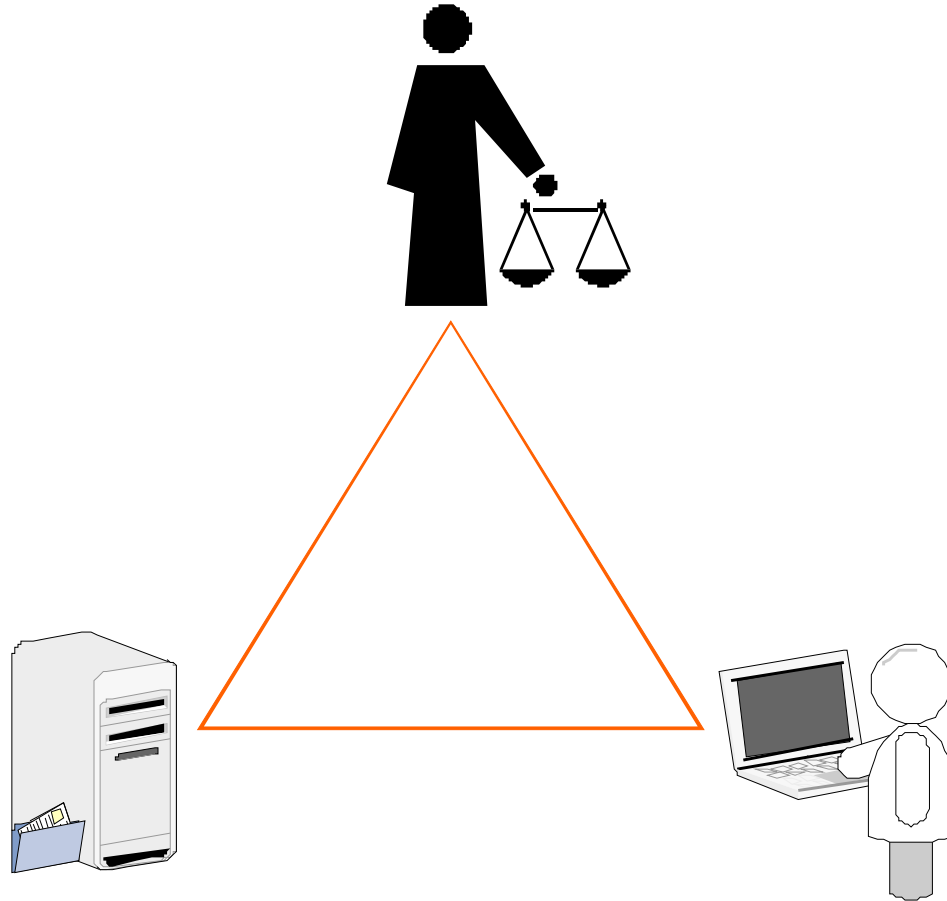
- Customers
- Branch offices
- Partner offices



Our customers

- Computing and data center operators
- Internet service providers and backbone operators
- Telecommunications companies
- Supply chain operators
- Transport and logistics
- Internationally acting companies
- Banks and operators of financial networks (Clearing of credit cards)
- Producers of security hardware and software
- Public authorities and countries

IT-Administration



Initial position

- Usually conflicting priorities between
 - Management (legislation)
 - Administration
 - User
 - Technology
- Products promise heaven and earth
- Too little „Human-Resources“
- Too little time to "do it right"

Business Continuity



- Business critical application
- Availability => 99,995%
- On-Site Administration
- Remote administration needs to be possible

New demands

- **Sarbanes-Oxley Act**
 - USA 2002 ff
- **Basel II**
 - European Countries
- **KonTraG**
 - Corporate Sector Supervision and Transparency
- **TransPuG**
 - Transparency and Disclosure Act

SoX

- The Sarbanes-Oxley Act of 2002
- US federal that introduces new corporate board responsibilities
- Result of the corporate and accounting scandals of Enron, Worldcom etc.
- Named after its sponsors
 - Senator Paul S. Sarbanes (democrat)
 - Representative Michael Oxley (republican).

SoX

- *"The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting."*

Public Company Accounting Oversight Board
Auditing Standard II

Basel II

- *"International Convergence of Capital Measurement and Capital Standards - A Revised Framework"*
- Most important regulation for European financial service institutions
- Main aim: Improving consistency in the way in risk management of banks and banking regulators
- Mandatory within Europe since January 1st 2007, USA will follow in ~~2008~~ 2009 (probably)

KonTraG

- Corporate Sector Supervision and Transparency Act (KonTraG) enacted by the German Bundestag in 1998
- Became effective on May 1st 1998
- Aims to improve corporate governance in German companies
- KonTraG specifies and at the same time extends mainly regulations from the German Commercial Code (HGB, *Handelsgesetzbuch*) and the Stock Corporation Act (AktG, *Aktiengesetz*).
- KonTraG extends the liability within the company of
 - Corporate management
 - Board of directors
 - Financial auditorss
 - Managers

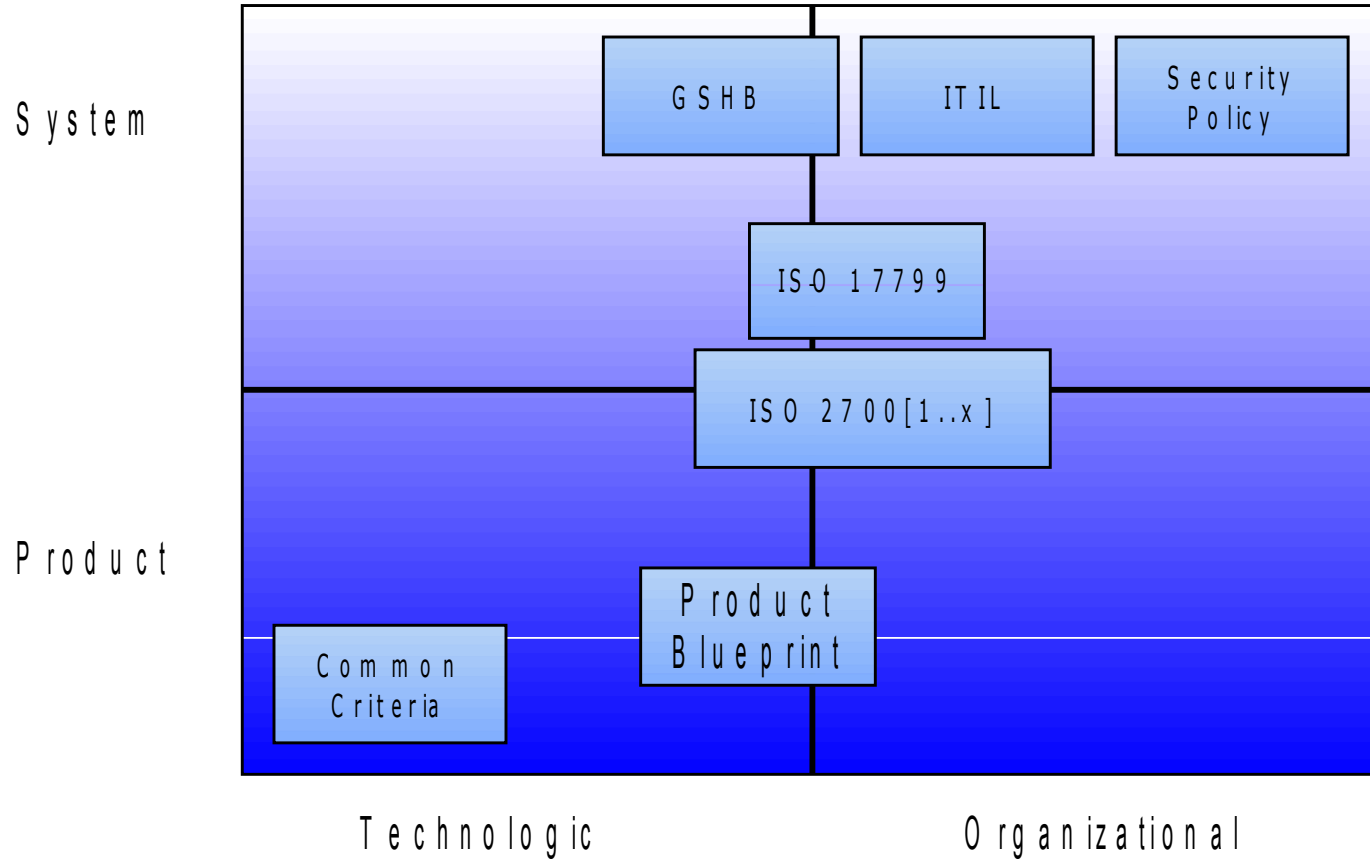
TransPuG

- Act reforming the German stock corporation and accounting law.
- Enacted by the Bundestag and Bundesrat in 2002 order to promote transparency and publicity
- TransPuG tightens accounting standards, risk management responsibility, and auditor accountability.

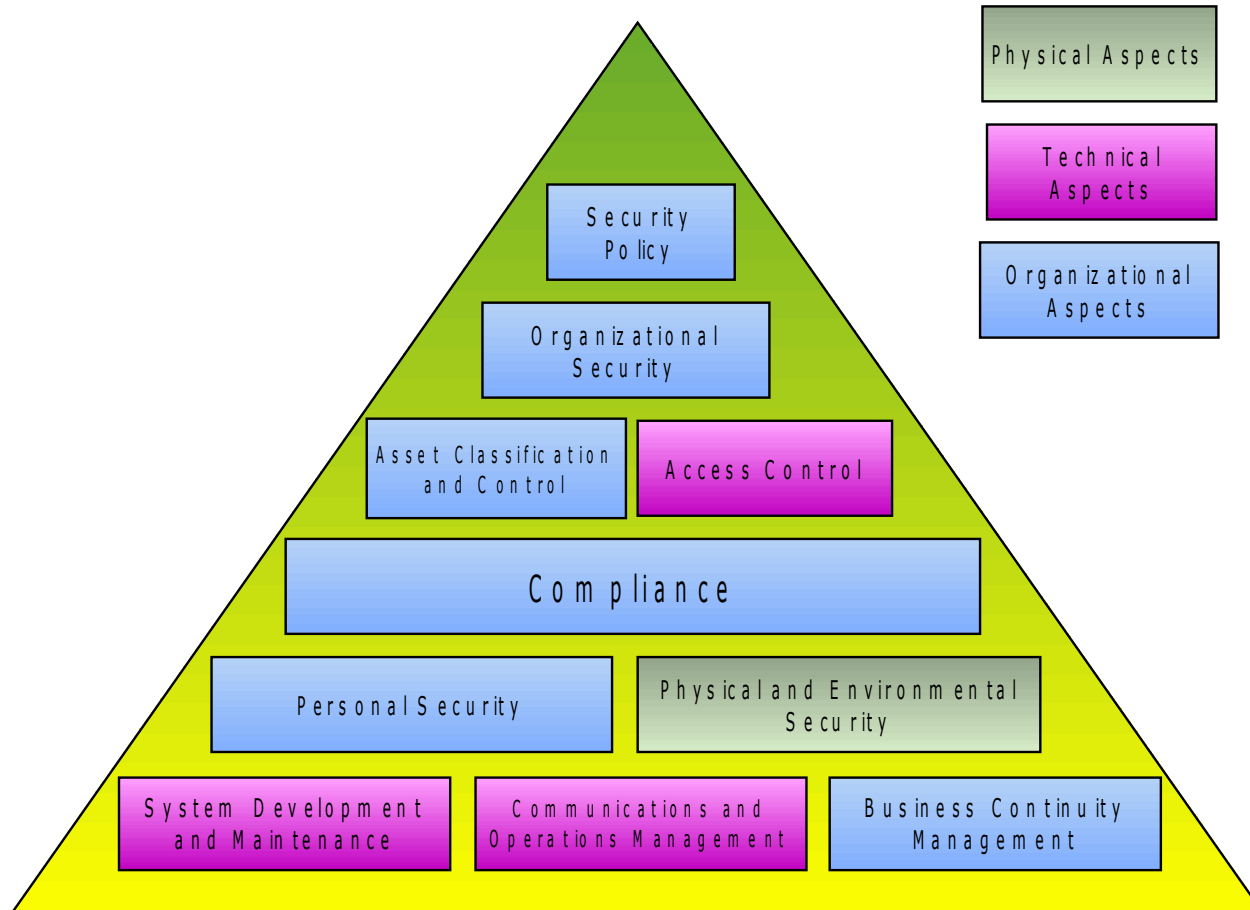
Blue or red pill?



Rules, but which?



BS 7799:2005



Non only technology

- Security is not a product!
- Processes must be implemented
- Audits and cycles are important

Organizational

Technology

And Linux ?

- Linux offers standardized interfaces
 - Syslog
 - SNMP v3 (Traps/Informs)
 - IP-Tables
 - Kernel logging
 - SE-Linux
 - App-Armor
 - LDAP, PAM, Identity Management, PKI

Security Framework

- Set up auditable structures
- Documentation on policies and procedures
 - ISO 2700x and ITIL provide "high level" framework
 - Blueprints and technical guidelines on a parameter level
- Use standard tools "Out-of-the-Box"

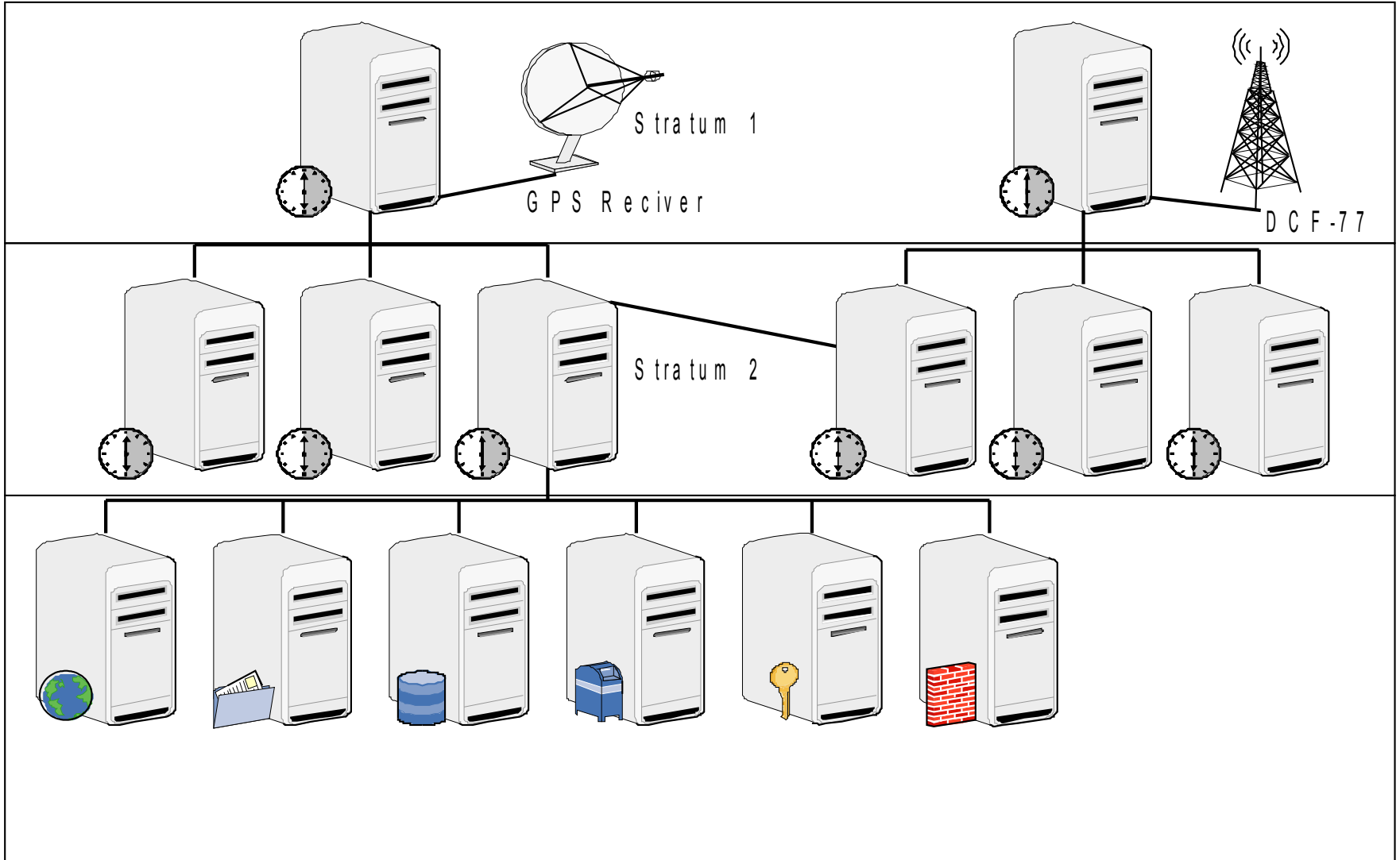
What to do

- Do not set up data sinks
- Zero administration **never** works
- Don't want too much at the same time
- Provide resources for data analysis

Log Results

- Synchronize time at all monitored servers
- Continuous structures can be set up using:
 - NTP
 - RRD-Tool performs quality control on NTP
- HA systems with NTP clusters
- Use several redundant time sources
- Encryption of timestamps (optional)

NTP Concept



Logging

- Record system messages such as
 - Login data
 - Abnormal daemon behavior
 - Security relevant messages
- Violations of firewall rules
- Other security relevant events
- Syslog-NG can sign messages, securing them against manipulation

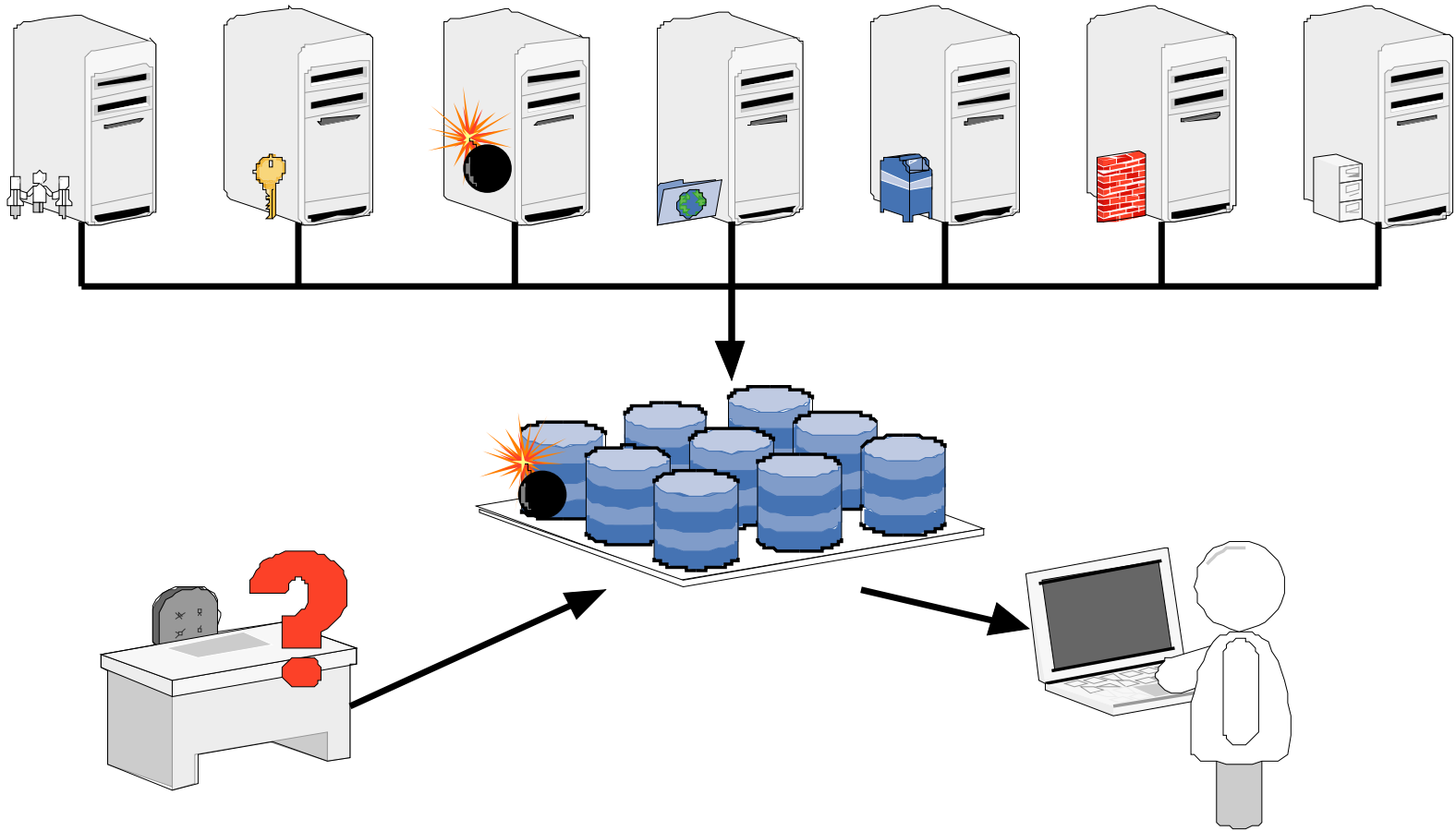
"Paper is patient"

- Log files are too large to be evaluated line by line
- High personnel expenses
- Automated evaluation vs. manual
- Tools such as Logwatch help

Data Analysis

- Escalation plan for suspicious messages
- A Security ticketing system can help
 - Example: OTRS
- Every unknown message automatically opens a new ticket
- If a ticket is not processed promptly it is escalated to the next instance

Concept



Further sources

- Viruses – protection from malware
- Content Security (SMTP, HTTP, Floppy, USB-Memory ..)
- Patch and update management

HIDS and NIDS

- Host and network intrusion detection systems
 - Creation of policies is very complex and time consuming
 - Abnormal network traffic should be detected
 - Manipulations of the operating system should be detected
 - Useless without configuration, permanent management and customization

Research & development

- Honey pots can help in certain areas
- Use existing data first
- Early warning systems can help with Basel-II and KonTraG.
- The main effort is documentation and implementation, not the software costs

Questions ?



Thank You



dn
Systems

DN-Systems GmbH
Hornemannstr. 11-13
31137 Hildesheim, Germany
Phone: +49-5121-28989-0
Mail: info@dn-systems.de

DN-Systems International Limited
P.O. Box 500 581
Dubai · U.A.E.
Phone: +971-50-2861299
Mail: info@dn-systems.com