Fachhochschule
Gelsenkirchen

Internet Early Warning System
→ Basis

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is)
internet security.

Content

- Aim and outcomes of this lecture
- Motivation of
  Internet Early Warning System (IEWS)
- Targets of IEWS
- Structure of IEWS
- Process of IEWS
- Different realization of IEWS
- Summary

Content

- **Aim and outcomes of this lecture**
- Motivation of Internet Early Warning System (IEWS)
- Targets of IEWS
- Structure of IEWS
- Process of IEWS
- Different realization of IEWS
- Summary

Internet Early Warning System
→ Aims and outcomes of this lecture

Aims

- To introduce the motivation and the target of an Internet Early Warning System for the different stakeholder
- To explore the structure of an Internet Early Warning System
- To analyze the processes of an Internet Early Warning System
- To assess the need of an Internet Early Warning System

At the end of this lecture you will:

- Understand the meaning of an Internet Early Warning System.
- Know the basic structure of an Internet Early Warning System.
- Understand how the processes could be.
- Understand the problems that arise by developing an Internet Early Warning System.

Content

- Aim and outcomes of this lecture
- **Motivation of Internet Early Warning System (IEWS)**
- Targets of IEWS
- Structure of IEWS
- Process of IEWS
- Different realization of IEWS
- Summary

Motivation
→ The object „Internet“

- **The usage of the object “Internet” is increasingly growing**
  - Increase of the number of Internet users in Germany from 6,5% in 1997 to 57,6% in 2006 [1]
  - 94 % of the German enterprises have access to the internet (2006)
  - Worldwide there are about 16 % of the population online (2006)

- **Evolution from a platform for the exchange of Information to a platform for multiple services**
  - Wikipedia
  - Amazon / Ebay
  - E-commerce turnovers have doubled from 2006 to 2008 [1]

=> **The Internet is a critical infrastructure resource**

Motivation
→ Challenges

- The **Internet** has become a **large and complex** IT system which goes beyond
  - all geographical,
  - political,
  - administrative and
  - cultural borders
    leaving a new and **unusual challenge to our society**.

- The **Internet is not regulated** and consists of self-governed Autonomous Systems (AS) each managed by individual organizations mostly part of the private sector.

- The **threat** in this area has not been reduced, but it **has become more present** over the last view years.

Motivation
→ The Internet and Security (1/4)

- The FBI estimates that a **damage of over 80 billion USD** is annually caused to US-Enterprises by attacks and misusage of IT-infrastructure [1].
- The worldwide **expense for IT security** grew from about 28 billion USD to **about 54 billion USD** from 2002 to 2006.
- Survey of the German Federal Office for Information Security (2006) [2].
  - **Expertise** in the area of IT security **is not widely spread** among internet users
  - Every second participating **user** of the survey **works and surfs with root privileges**
  - Enterprises have identified the need, but only **about a fifth has security guidelines**

Motivation
→ The Internet and Security (2/4)

- Survey of the German Federal Office for Information Security (2006) [2]
  - Only two thirds of the employees are familiar with these security guidelines
  - Prevalent form of security incidents
    - Zero-Day-Exploits, Trojan Horse, Viruses, Worms, Spyware/Adware, DDoS-Attacks, unwanted e-mails, Bot-networks, Phishing, Identity theft / Social Engineering, Dialer, Ping-Calls, insider threat
  - Growth of the discovered security vulnerabilities from 2005 to 2006 by 40 %
  - Total amount of SYN-Floods increased from 2004 to 2005 by 680 %
  - 80 % of all e-mails are spam

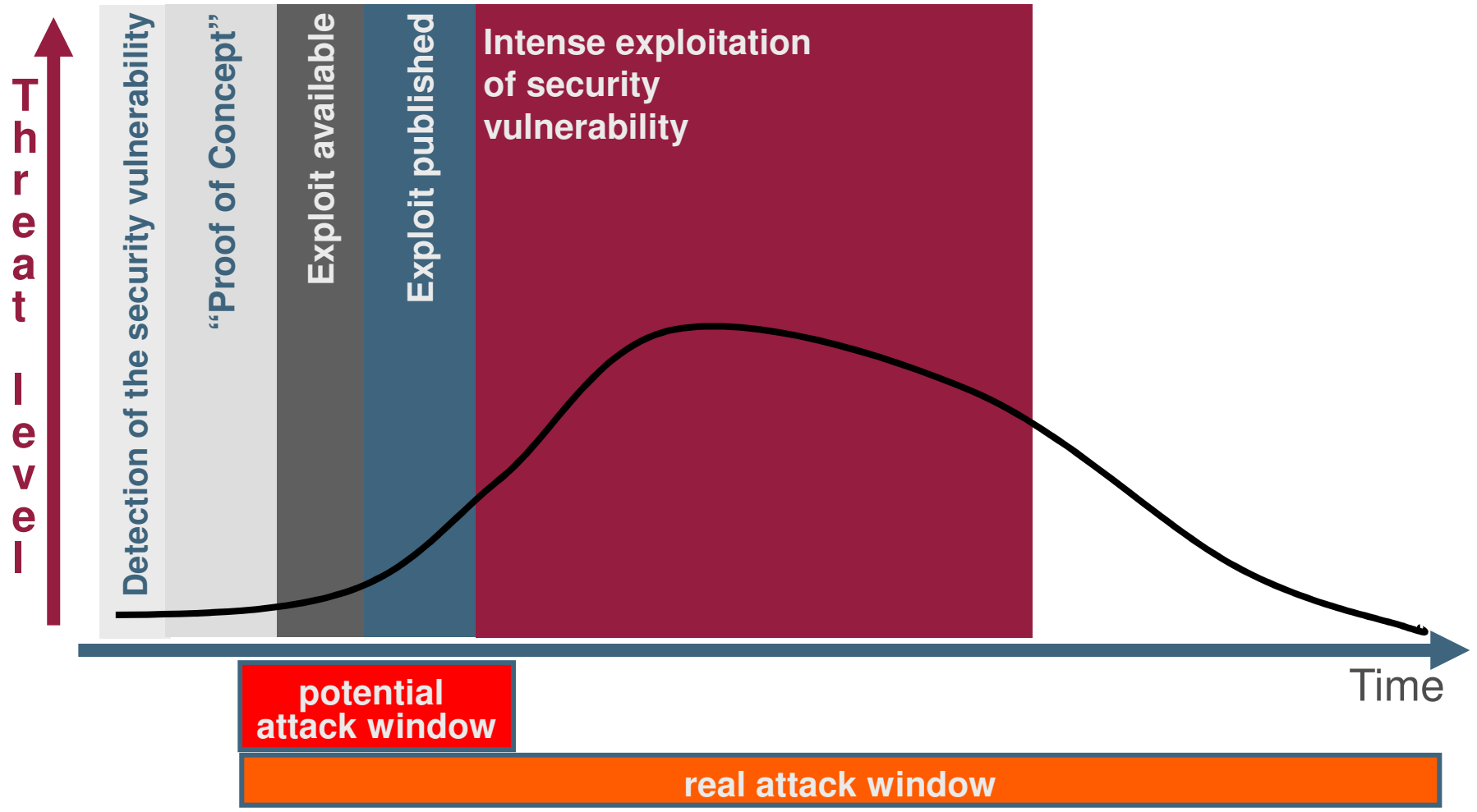
Motivation
→ The Internet and Security (3/4)

- Survey of the German Federal Office for Information Security (2006) [2]
  - Technology with a high risk potential
    - VoIP, WLAN, mobile phone / smart phone / PDA, AJAX, process control systems, RFID

- **Methods used for more security**
  - Firewall, IDS, IPS, honey pots, virus scanners, anti-spam
  - Deliver information about security incidents within the network they are installed in
  - Control the boarders of the network and the communication within the network.

Motivation
→ The Internet and Security (4/4)

- More security vulnerabilities due to more complex IT systems
- More rapid development of malware and exploits

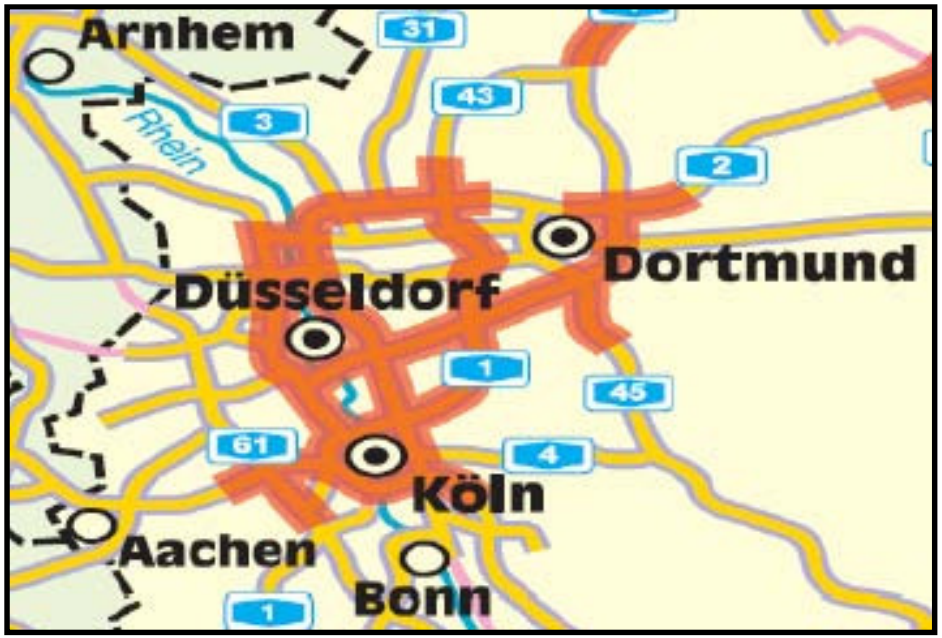


Motivation
→ Analogy (1/2)

Local View

Motivation
→ Analogy (2/2)

Global view



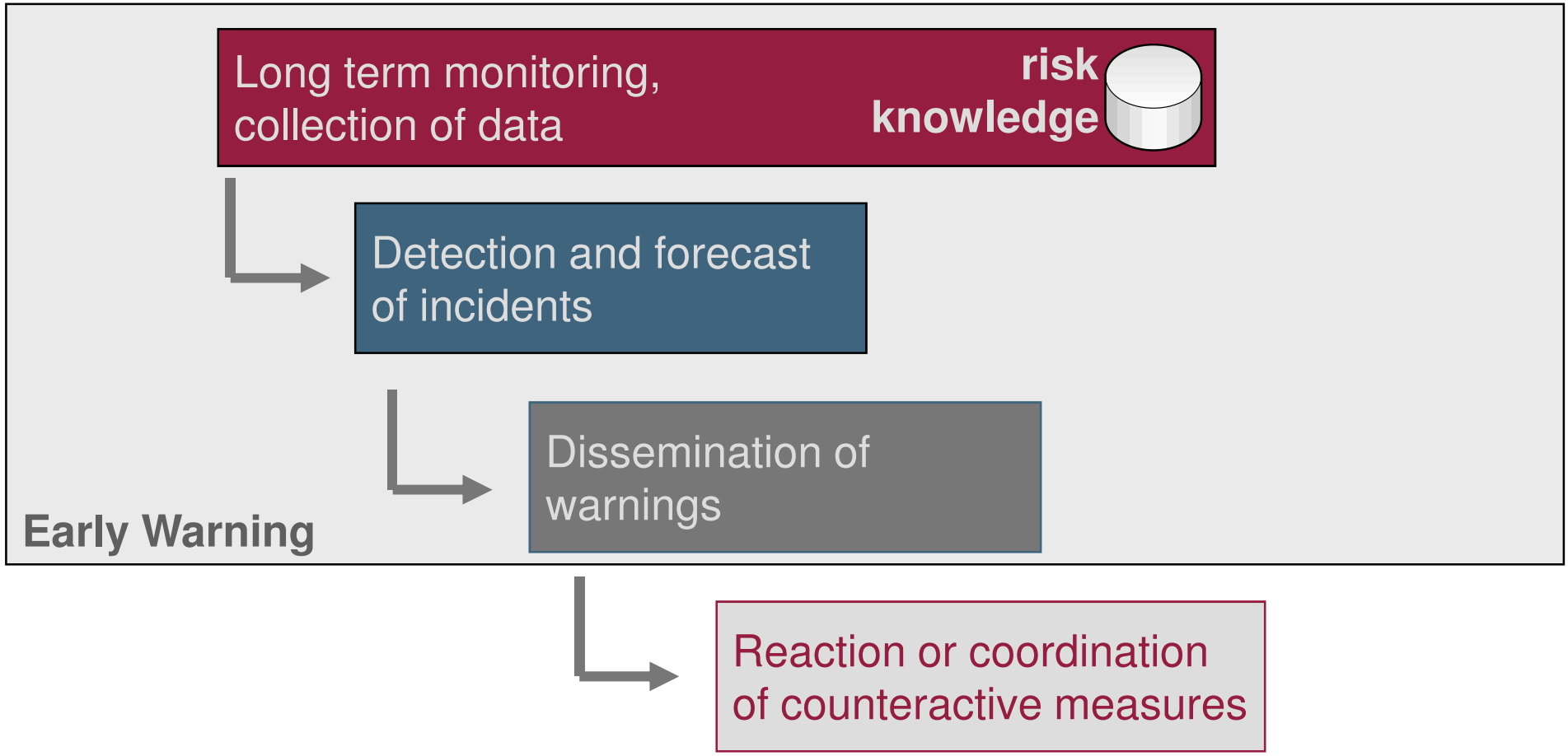
Air Traffic Control

Motivation
→ Terms

- **The Term: Warning**
  - *"A warning is a prediction of a damage which might possibly occur, but which might still be prevented or reduced. It drives the attention towards an imminent danger." [3]*

- **The Term: Early Warning**
  - *"A successful early warning is a warning of threatening natural incidents which comes in time, so that the potentially affected has the chance to react und therefore to prevent or reduce the damage caused to persons and property." [3]*

Motivation
→ Warning process



- Early warning is part of the risk management and of national homeland security systems, which protect a national territory from all sorts of natural and man-made hazards

Motivation
→ Conclusion

- The **Internet and Security**
  - A detailed view on the current situation (situation awareness) is only possible for the operator within his own network.
  - Information about the situation of the rest of the internet are very difficult to collect!

  => There is a lack on information to establish an internet situation awareness

  => Early reaction towards threats is not possible or only in a very limited fashion

=> **What we need is an Internet Early Warning System to assess the global view of the security status of the Internet**

Content

- Aim and outcomes of this lecture
- Motivation of
  Internet Early Warning System (IEWS)
- **Targets of IEWS**
- Structure of IEWS
- Process of IEWS
- Different realization of IEWS
- Summary

Internet Early Warning System
→ Targets

- **Strongly improve** and **develop** the **security** and **trustworthiness** of the used IT infrastructure of the **internet** in a **resistant fashion**

- To establish this, information about the **status** of the IT infrastructure is **continuously generated** and evaluated by means of an Early Warning System and in cooperation with public and private partners

- In addition, efficient reactions on incidents will be - preferably automated - initiated and implemented by all partners

Targets of Early Warning Systems
→ Public Private Partnership (PPP)

- **Trustworthy collaboration** between public and private partners in the area of IT security.
- Work together to **establish a higher level of security and trustworthiness** of the common IT infrastructure of the Internet.
- **What is important?:**

If you can't measure it, you can't manage it!

- The IT infrastructure of the Internet can only be **measured** and **managed** in **collaboration**, therefore a public private partnership is not just reasonable but also neces!ary.

Internet Early Warning System
→ A possible definition: IEWS

- Based on a **reliable** findings about
  - **threatening** or
  - already **occurred IT security incidents**, which preferably only **involve few concerned**,
- an **IT security situation awareness** will be updated continuously
- and in the case of
  - an adequate **relevance**
  - a **qualified warning** will be disseminated
  - to the **potentially concerned**,
  - to **avoid** or **reduce** their estimated **damage.**

Targets of Early Warning Systems
→ Functional requirements (1/3)

- **Detection of Attacks**
  - At an early stage, best before actual damage is caused
  - … but always early enough to minimize the potential damage.
  - Known and unknown attacks
- **Support** in the **decision making process** and in the **development of counteractive measures**
  - Tools for analyzing and to display results
  - Decision-making aid by the use of expert systems
- **Assistance in the collection of evidence (forensic)**
  - Collection of evidence of a later legal reaction

Targets of Early Warning Systems
→ Functional requirements (2/3)

- **Monitoring of the development of Internet traffic**
  - How is the Internet traffic going to develop?
  - How does the infrastructure have to be extended?
  - Which technologies will gain or loose importance in the future?

- **Creation of a IT security situation awareness**
  - Overview over all security relevant incidents
  - Appropriated method for visualization the IT security situation awareness

Targets of Early Warning Systems
→ Functional requirements (3/3)

- **Further requirements for an Internet Early Warning System**
  - Reliability
  - Security of the System towards attacks
  - Ensuring privacy and protection of confidence
  - Maintainability
  - Expandability
  - Performance / Scalability

Targets of Early Warning Systems
→ Asymmetric threatening

- Most attacks are carried out globally and not linked to one specific location (e.g. DDoS instead of DoS with the help of botnets).
- The reaction on a security incident is always just initiated locally.
- The effort is multiplied by the number of victims, which all have to perform the same effort to reduce and to eliminate the damage.
- Purpose of an Internet Early Warning System is to initiate **efficient reactions** on incidents with all partners preferably in an automated fashion.
- **This bundled effort will highly increase the effect of the measures against the attack**.

Targets of Early Warning Systems
→ Qualified Early Warning (1/2)

- **Qualified Early Warning**
  - Timely **information on IT security incidents** (attacks), which could cause damage.
  - Fast and high quality **information on recommended actions**, which can be used to assist the prevention or reduction of damage caused by an attack.

- **Optimal quality** of Early Warnings for the IT should be established by the cooperation of IT security experts.
  - ***Faster protection,*** by the means of fast and collective detection of attacks.
  - ***Reduced damage***, by the means of collective actions.
  - ***Economic risk management,*** by the means of an evident IT security situation awareness of the commonly used IT infrastructure of the internet

Targets of Early Warning Systems
→ Qualified Early Warning (2/2)

- Advantages of qualified Early Warnings for the IT are:
  - The individual partners receive **hints on attacks** with **sufficient relevance**, which sporadically take place towards the other partners' infrastructures but so far not towards the own infrastructure.
  - This can be used by the not effected partners to have an **early start** on taking **efficient counteractive measures** to prevent or reduce potential damage.
  - The initiation of **collective counteractive measures** has a much wider effect against attacks.
  - The **security and trustworthiness** of the common IT infrastructure of the Internet can be **raised sustainable** by the means of collective qualified Early Warnings for the IT.

Content

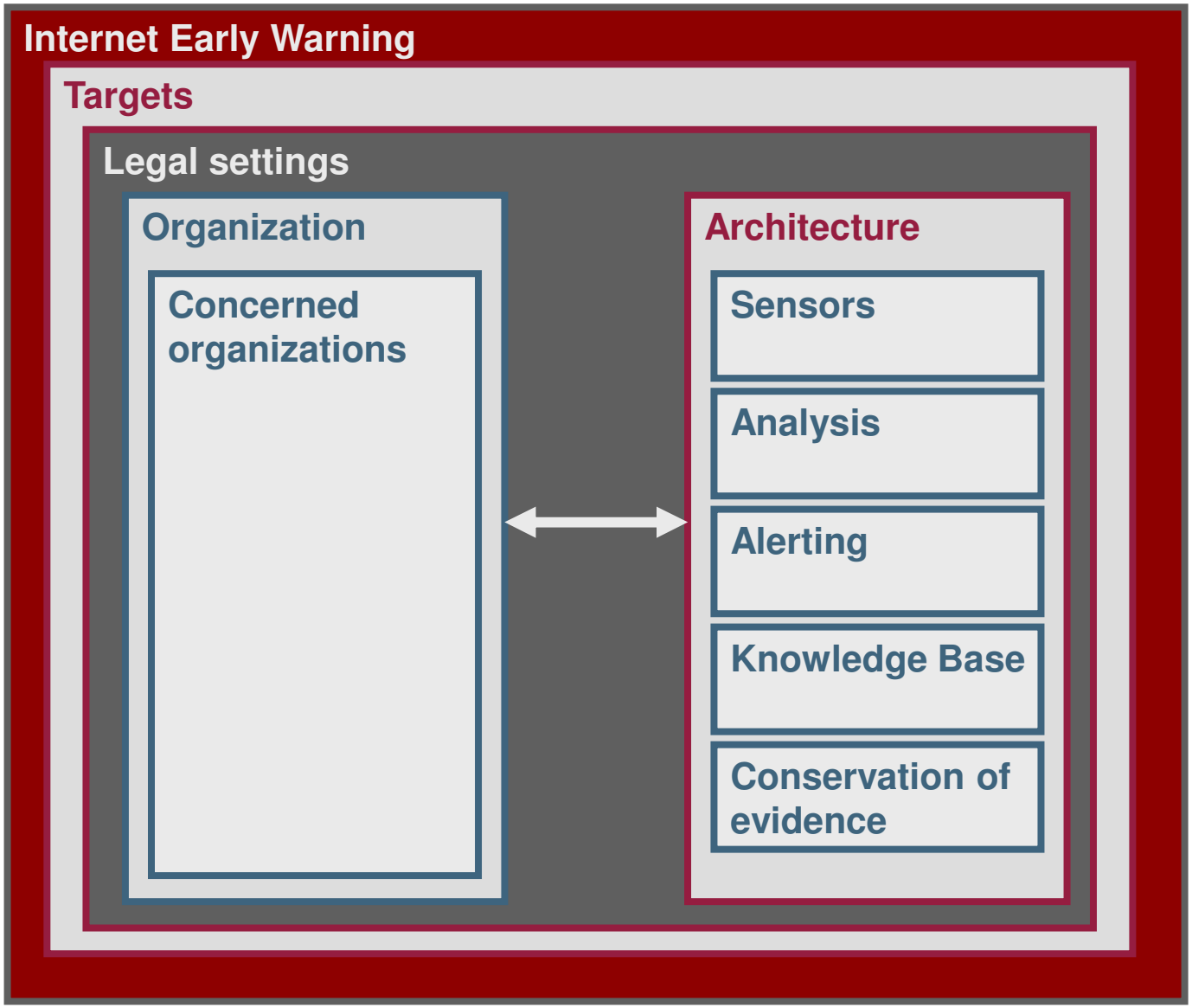
- Aim and outcomes of this lecture
- Motivation of
  Internet Early Warning System (IEWS)
- Targets of IEWS
- **Structure of IEWS**
- Process of IEWS
- Different realization of IEWS
- Summary

Structure of an Early Warning System → General (1/2)

- An Internet Early Warning System (IEWS) consists of a **number of components**

- An Internet Early Warning System differs depending on the “environment”
  - **Targets to be achieved** by the use of an IEWS
  - **Legal conditions**
  - **Partners participating** in development and operation of an IEWS

Structure of an Early Warning System
→ Model



Structure of an Early Warning System → Abstractly phrased

$$EWS = (N, P, O, L, T, E)$$

with:

- EWS := Early Warning System
- N := **N**etwork, which are monitored
- P := Participant
- O:= **O**rganization, definition of the relations of the concerned and of the processes
- L := **L**egal framework, which are relevant for operation
- T := **T**argets, which are aimed to be established by the use of an Early Warning System
- E := technical **E**lements of the Early Warning System

Structure of an Early Warning System → Element: Network (N)

- The Network that ought to be observed
- In this case the Object “Internet” consisting of various autonomous systems
- Important due to different aspects
  - Distribution of the sensors
  - Spreading of failures
  - Conducting of counteractive measures
- Open Questions
  - How can the structure of the network be captured?
  - On which level of abstraction should the network be described?
  - Which are the most important nodes?

Structure of an Early Warning System → Element: Participant (P)

- Set including the participating organization (that are **involved in the early warning activities**
- Distinction between those involved actively and those involved passively
- Those participating organizations in an **active role** take part in the development and operation of the Early Warning System
  - Sensor operators, Operators of assessment centers and supporters for the implementation of counteractive measures
- Those participating organizations in a **passive role** use the gathered information, but are not participating in the operation of the system
  - Private end-users, enterprises, ...
- Participating organizations have their **individual interests** for supporting Early Warning Systems
  - These individual interests may be in conflict to those of others
  - The set of the targets that are aimed to be reached with an Early Warning System is a subset of the set of individual interests of all participating organizations

Structure of an Early Warning System → Element: Organization (O) – (1/2)

- Organizational structure of the Early Warning System
- Organizational and operational structure

$$O = (O_{Operational}, O_{Organizational})$$

- **Organizational structure**
  - Definition of the organizational units
    - Sensor operator, assessment centers, CERTs, operators of critical infrastructure
  - Definition of the relations between these units
  - Definition of the responsibility of the units

Structure of an Early Warning System → Element: Organization (O) – (2/2)

- **Operational Organization**
  - Definition of the processes for the operation
    - Reaction in case of an incident
    - Flow of information between organizational units

- **Important aspects**
  - Short decision processes
  - Efficient paths for information flow
  - Strictly defined responsibilities

Structure of an Early Warning System → Element: Legal framework (L)

- The legal framework have an influence on the operation of an Early Warning System
- Depending on the legal situation the operation might be subject to more or less limitations
- Relevant areas of the law
  - Privacy (data protection)
  - Protection of confidence
  - Law of contract
- The legal framework sometimes define the ability of an Early Warning System to reach the aimed targets

Structure of an Early Warning System → Element: Technical Elements (E)

- Technical Elements of an Early Warning System

$$E = (S, A, AL, KB, CE, AR)$$

  - S := Sensors
  - A := Analysis
  - AL := Alerting
  - KB := Knowledge Base
  - CE := conservation of evidence
  - AR := Architecture

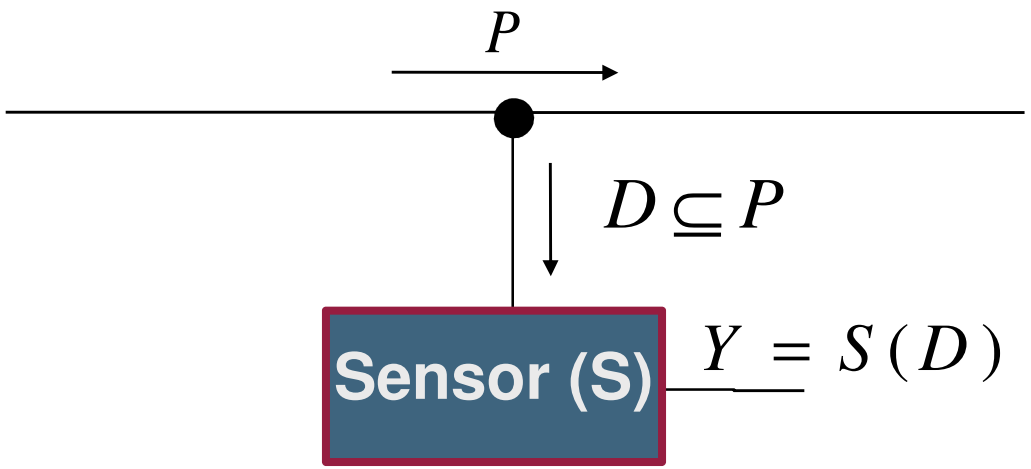
- The interaction of these technical elements offers the functionality of an Early Warning System

Structure of an Early Warning System → Technical Element: Sensor (S)

- Sensor collects data, which is used to determine the current status
- Sensors are distributed throughout the entire Network (N), to gain a representative overview of the network
- Different types of sensors have been developed
  - Complete recording of the network traffic (e.g. Wireshark)
  - Netflow (Router)
  - Packet based sensors (statistical)
  - Honeypots
  - Availability of Services, Nodes and Components
  - LogData analysis,
  - …
- Privacy and protection of confidence are important aspects
  - Use of methods for pseudonymisation and anonymization

Structure of an Early Warning System → Technical Element: Sensor (S)

- General view on a sensor connected to a communication infrastructure used to transfer data packets



  - with
    - P:= complete data traffic
    - D:= data traffic going through the sensor
    - Y := result of the processing conducted by the sensor
  - For the information content can be applied: $I(Y) \leq I(D) \leq I(P)$

Structure of an Early Warning System → Technical Element: Analysis (A)

- Core of an Early Warning System!
- Identification of security relevant incidents and alerting of the relevant authorities
- Monitoring of the development of the data traffic
  - Development of the Infrastructure
- **Configuration of the analysis element**
  - ***Subsymbolic level***
    - Evaluation of data concerning the current operating condition of the network
    - Identification of abnormal or security relevant incidents
    - Misuse und Anomaly Detection
    - Generates events, that can further be processed

Structure of an Early Warning System → Technical Element: Analysis (A)

- Configuration of the analysis element
  - ***Event-driven level***
    - Correlation of the identified incidents
    - Including further Information from external non-technical sources (e. g. CERTs, ...)
    - Generating Alerts if necessary
  - ***Learning Element***
    - Adjustment of the algorithms used for analysis an basis of the so far generated results
    - For example to adjust the algorithm to the changing network traffic, after a new service has gone online
  - ***Knowledge Base***

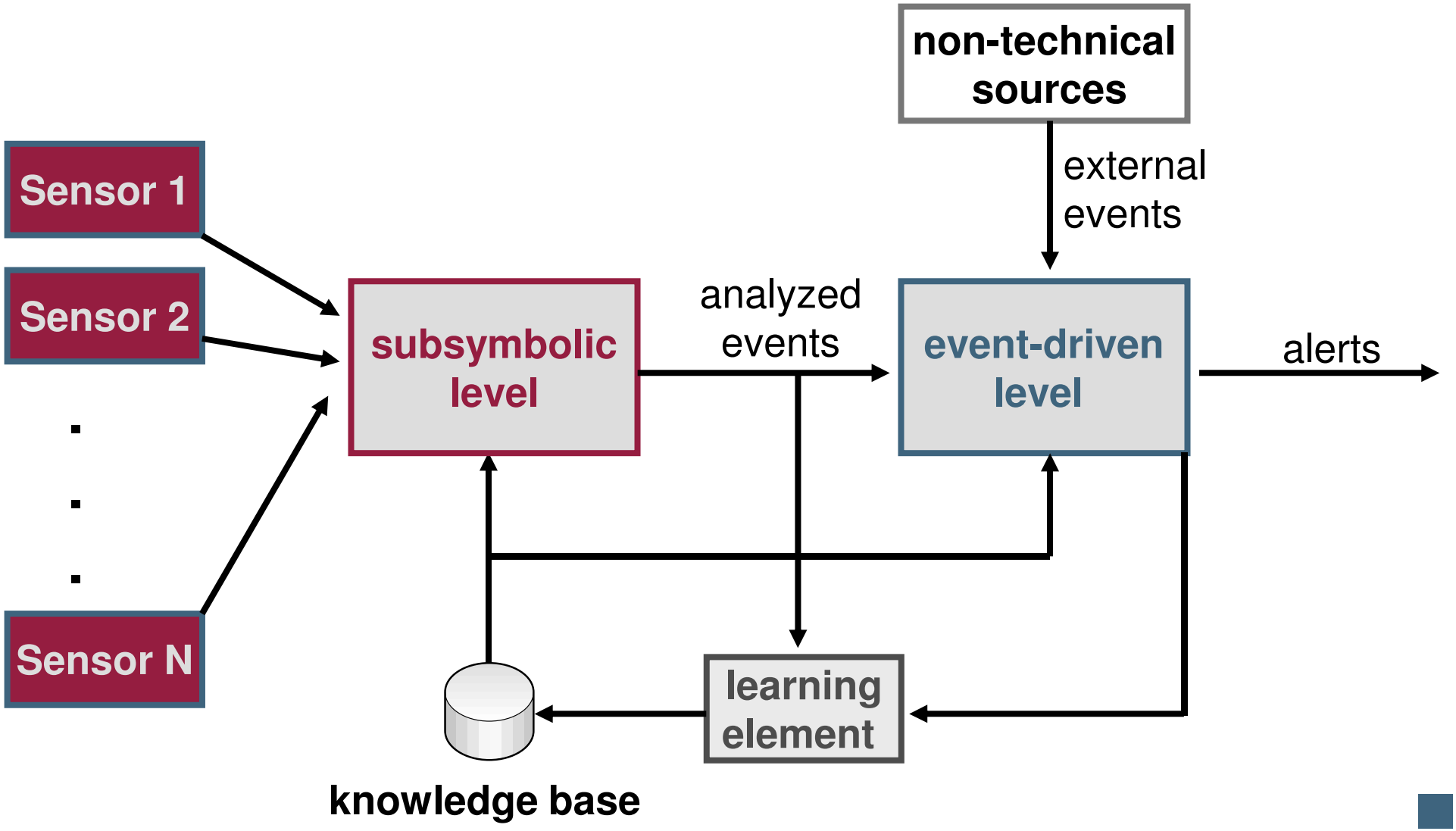
Structure of an Early Warning System → Technical Element: Analysis (A)

- Internet Early Warning Center at the Institute for Internet Security

Structure of an Early Warning System → Technical Element: Analysis (A)

- ***Problems***
  - huge amounts of data
  - Detection of unknown deflections and developing trends

Structure of an Early Warning System
→ Technical Element: Analysis (A)



Structure of an Early Warning System
→ Technical Element: Knowledge Base (KB)

- Knowledge about the environment
- Information about
  - normal state of the network traffic
  - Definitions / signatures of attacks
  - Counteractive measures
  - Proceedings when “problems” occur
- Needs to be updated frequently
  - Automated generation of virus-/attack-definitions (signatures)
  - Update of the “normal state” of the Network traffic
  - Solutions for so far unrecognized problems
- **Problem:** gathering of knowledge

Structure of an Early Warning System → Technical Element: Alerting (AL)

- Dissemination and Management of the generated Alerts
- Supporting the people in charge for the handling by offering them the knowledge base
- **Expert System** component
  - Gives hints for the solution of **formerly known problems**!
  - Gives support when working on unrecognized problems
- Offers support when transferring Information back into the knowledge base

Structure of an Early Warning System
→ Technical Element: Conservation of evidence

- Safeguarding von evidence in case of an attack
- Shall enable legal prosecution
  - Attack has been performed …
  - Information on the attacker …
  - Damage caused by the attack …
- **Important aspects**
  - Privacy
    - Access to recorded data only in case of an actual incident
    - Protection of the personal data against misuse
  - Authenticity
    - Tampering must be impossible

Structure of an Early Warning System → Technical Element: Architecture (AR)

- Architecture in which the components are combined
- Different aspects have to be respected
  - reliability, maintainability, complexity, performance, data protection and confidentiality
- Predetermined: distributed sensors
- Possible approach for the architecture
  - Centralized
  - Decentralized
- On top of this a combination of both approaches in also possible

Structure of an Early Warning System → Technical Element: Architecture (AR)

- **Centralized architecture**
  - Besides the sensors all components are placed at one centralized operational unit
    - **pros**
      - Easy maintainability
      - Limited complexity
    - **cons**
      - Could result in performance problems
      - Centralized bodies are easier to attack (e. g. DDoS)

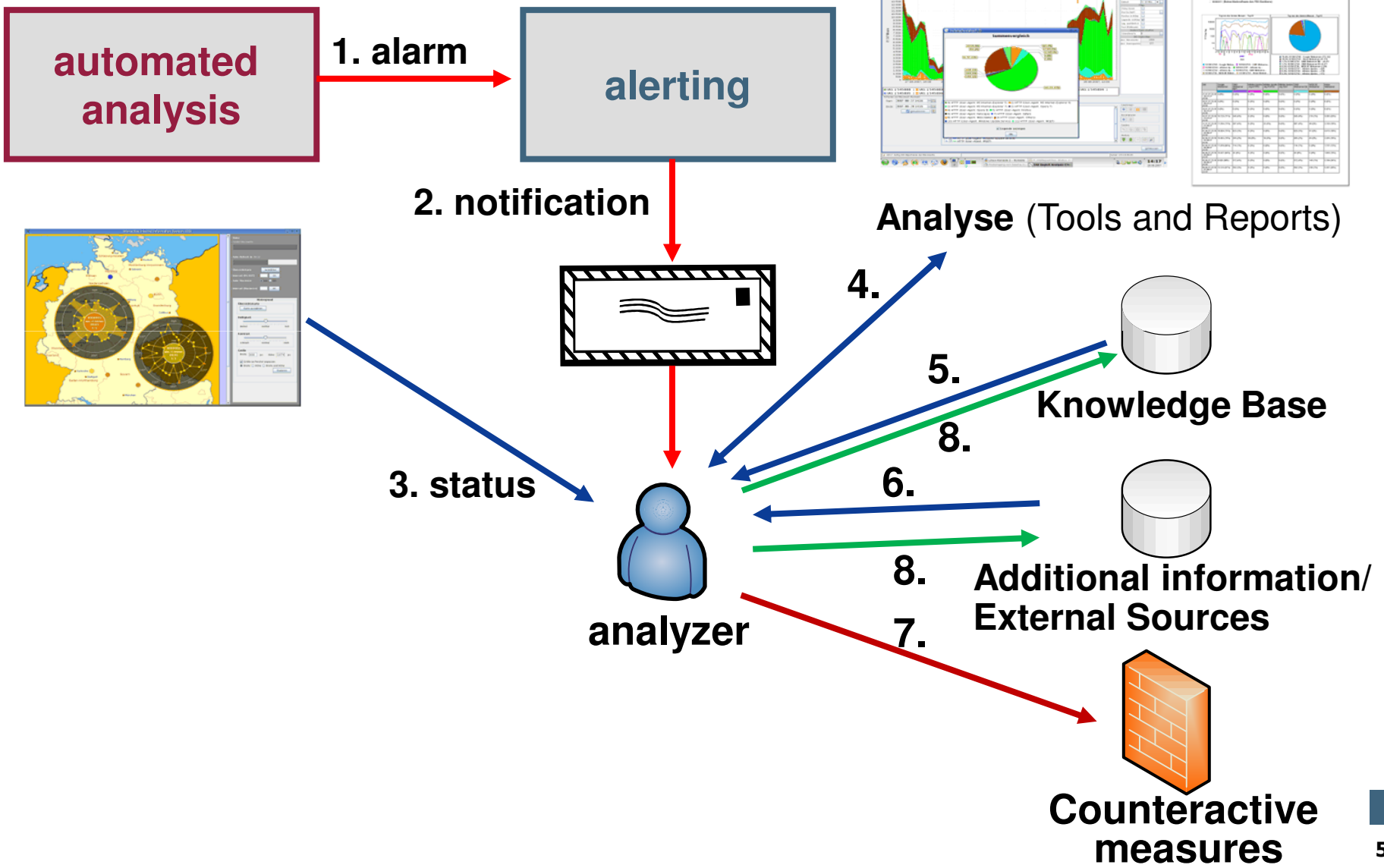
Structure of an Early Warning System → Technical Element: Architecture (AR)

- **Decentralized architecture**
  - Not just the sensors, but also the analysis component and knowledge base are distributed
  - Whenever necessary the individual components exchange information
  - Alerts can be disseminated from one centralized unit or by the different distributed units
  - **pros**
    - Performance
    - Not as easy to be attacked
  - **cons**
    - More complex
    - Maintainability not as good

Content

- Aim and outcomes of this lecture
- Motivation of
  Internet Early Warning System (IEWS)
- Targets of IEWS
- Structure of IEWS
- **Process of IEWS**
- Different realization of IEWS
- Summary

Early Warning Process



Early Warning Process

- 1. Security incident detected in data (alarm)
- 2. Concerned authorities are notified (e.g. e-mail)
- 3. See status (situation awareness)
- 4. Analyze the situation in more detail
- 5. Access to internal knowledge base
  - Hints for solving the problems
- 6. Access to further knowledge bases and external sources
  - Necessary, if local systems don't deliver enough information to solve to problem
- 7. Initiation of counteractive measures
  - Solving or reducing problem through counteractive measures
- 8. Update knowledge base and other sources
  - Newly generated knowledge, e.g. about problems or solutions to fix problems

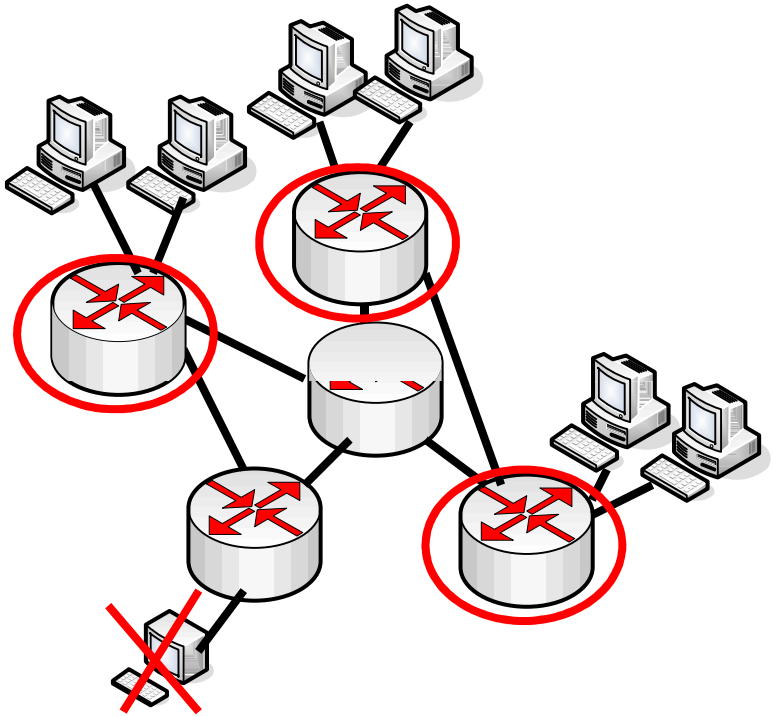
Early Warning Process
→ Possible reactions (1/3)

- **Private user / enterprises**
  - Reduction of the possibilities (firewall, …)
  - Increasing security mechanism
  - Selective shut-down (cut-off) of affected systems
    (without destroying evidence for possible criminal prosecution (forensics))
  - Complete deactivation of the uplink to the internet

- **Internet Service Provider**
  - Access Control Lists
  - Rate-Limiting
  - Blackholing
  - Off-Ramping / Sinkholing

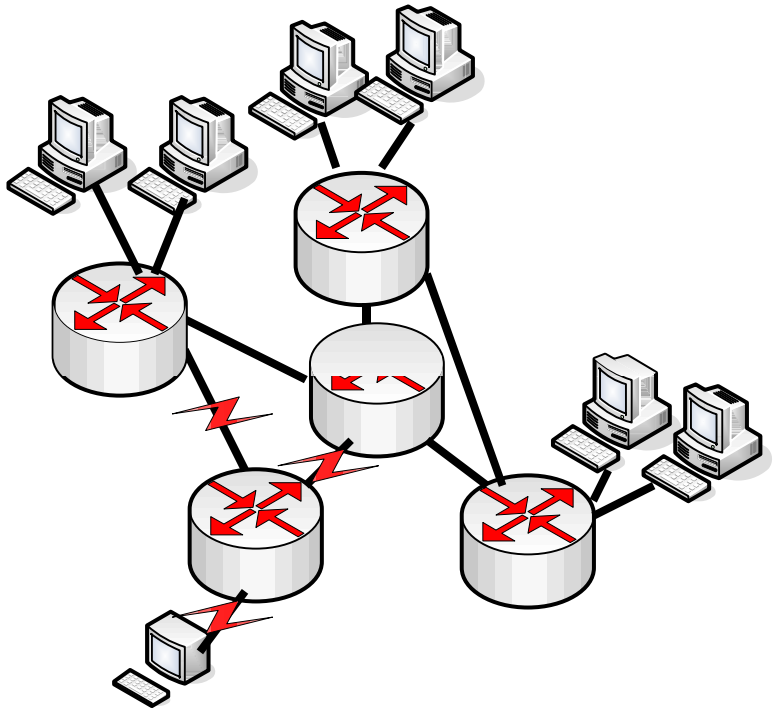
Early Warning Process
→ Possible reactions (2/3)

Access Control Lists

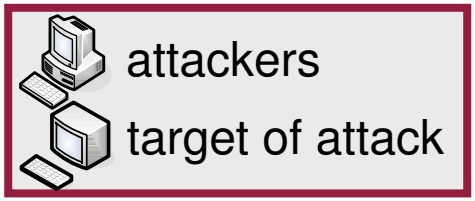


e.g. black-, white- or grey-List

Rate-Limiting

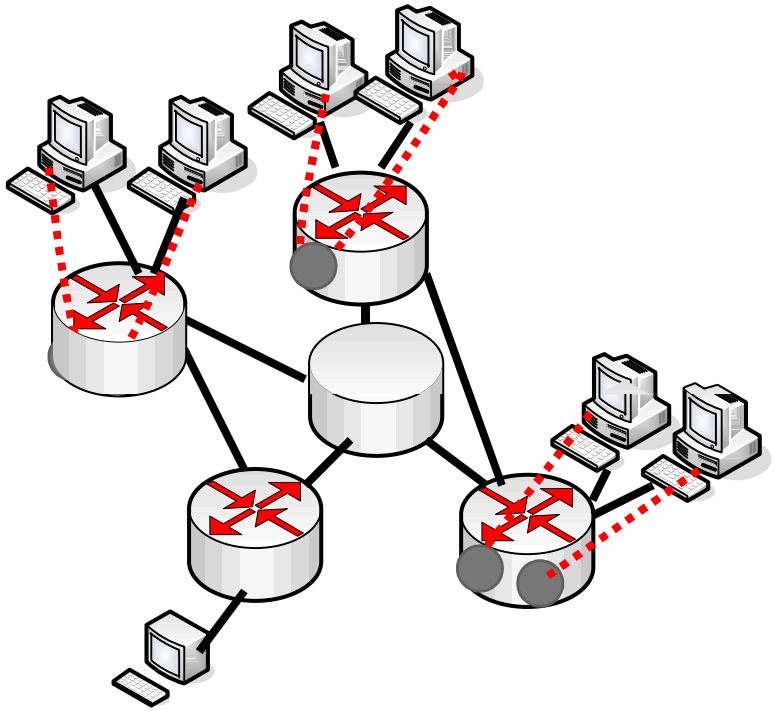


e.g. traffic shaping, packet shaping, bandwidth throttling, …



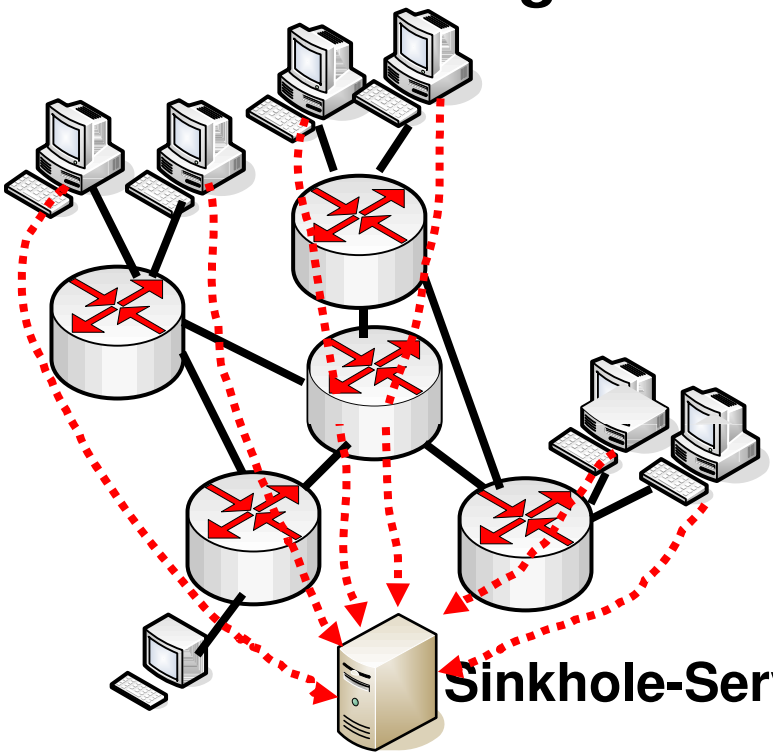
Early Warning Process
→ Possible reactions (3/3)

Blackholing



a null route (blackhole route) is a network route (routing table entry) that goes nowhere

Sinkholing



e.g. darknet (unused regions of IP address space), flow collectors, backscatter detectors, packet sniff…

attackers

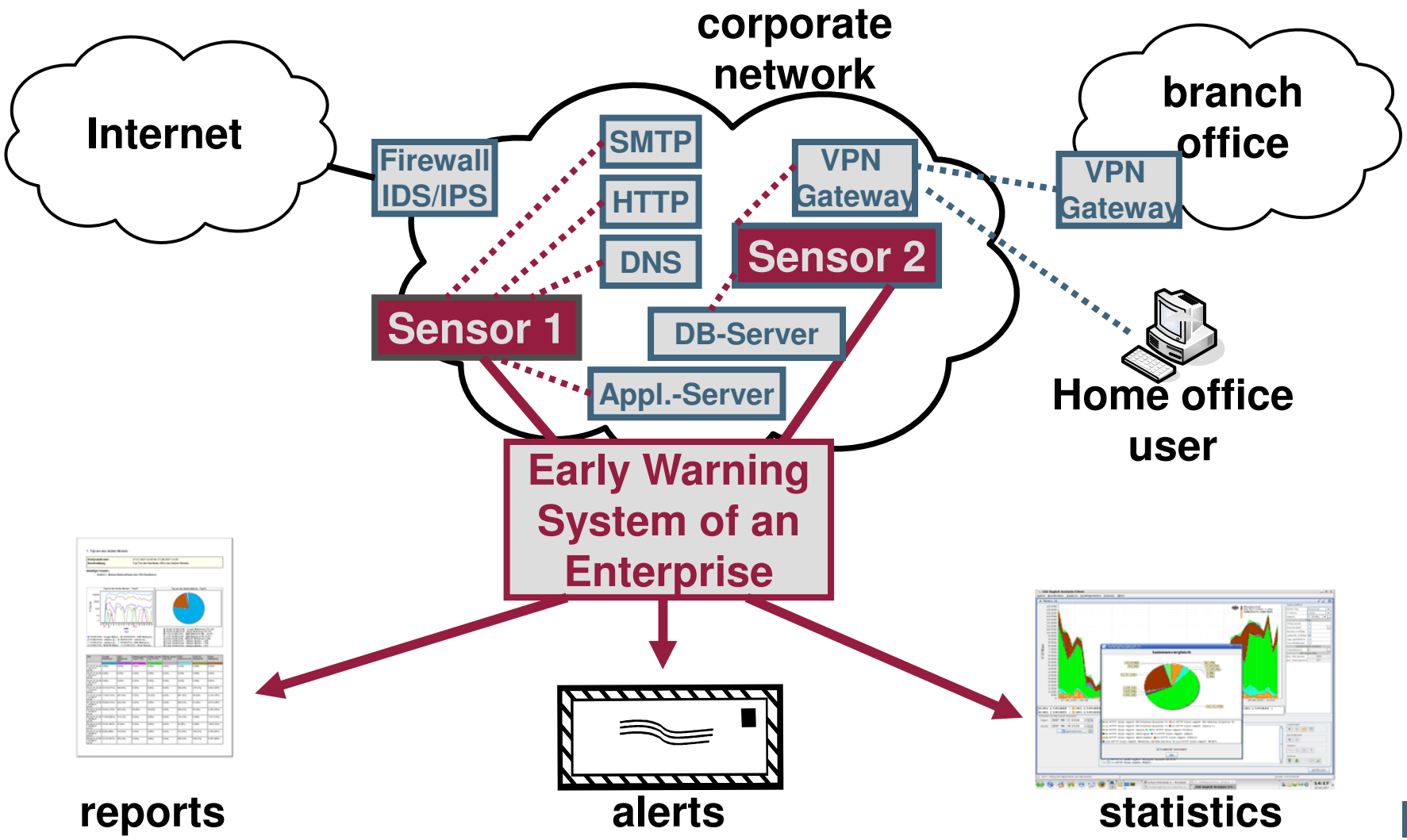
target of attack

Content

- Aim and outcomes of this lecture
- Motivation of Internet Early Warning System (IEWS)
- Targets of IEWS
- Structure of IEWS
- Process of IEWS
- **Different realization of IEWS**
- Summary

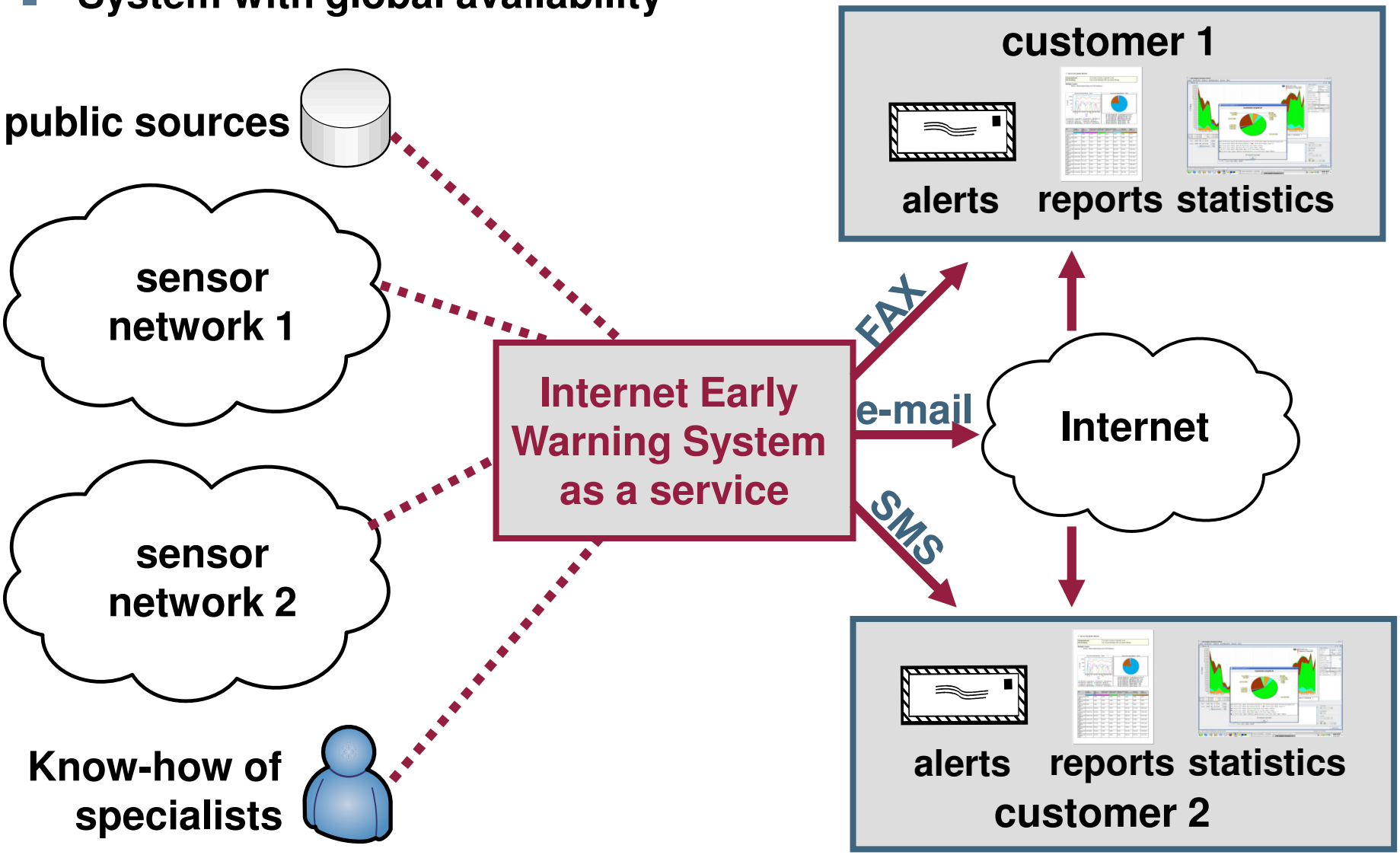
Methods of realization
→ Local installation

- Lokal installation



Methods of realization
→ System with global availability

- System with global availability



Methods of realization
→ Sensor View

- Many different types of Systems
  - Log data based Systems
  - Honeypot based Systems
  - Network traffic based Systems
- Next slides give a short overview of this systems (very short)

Methods of realization
→ Log data based Systems

- **Gathering of raw data from active components of the Internet**
  (router, switches, Intrusion-Detection- und –Prevention-Systems, firewalls, web servers, Honeypots, Security Appliances, etc.)
- **Analyzing of log files and protocol data**

```
Feb 12 16:26:49 ipcop kernel: INPUT IN=ppp0 OUT= MAC=
SRC=X.X.X.X DST=Y.Y.Y.Y LEN=64 TOS=0x00 PREC=0x00 TTL=44
ID=18033 DF PROTO=TCP SPT=2285 DPT=139 WINDOW=53760
RES=0x00 SYN URGP=0
```

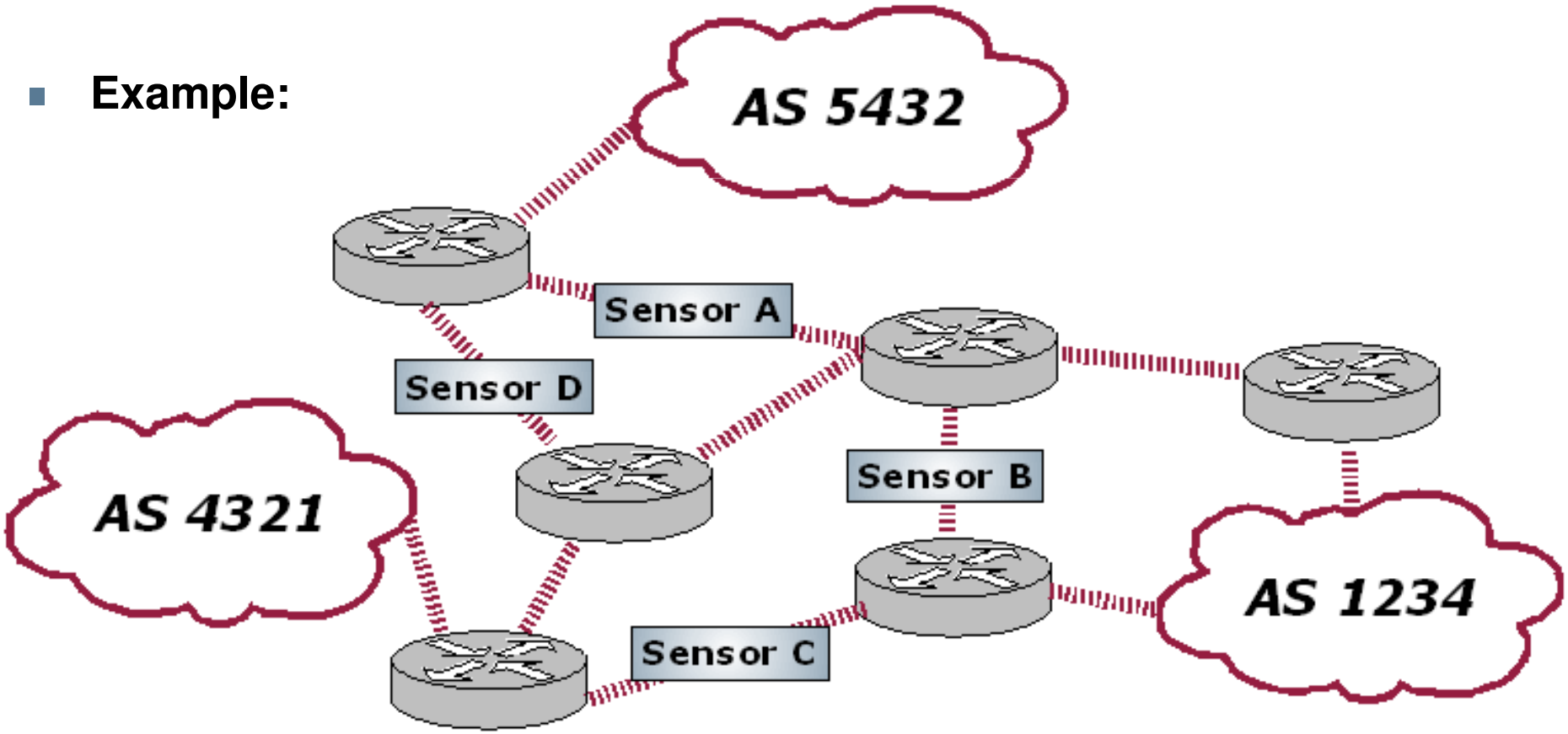
- **Analyzing of NetFlow und SNMP data**
  - Standardized formats for network flow and statistical data

Methods of realization
→ Honeypot based systems

- **Use Honeypots to gather information about**
  - Malware
  - Exploits
- **Gather no information about the actual network traffic**
- **Gives a deep inside in**
  - Malware activity
  - Exploits used
  - Attack strategies

Methods of realization
→ Network traffic based

- Collection of data with self-developed systems
- **Especially adapted sensor systems**
  analyzing of data packets, monitoring of QoS, availability check etc.
- **Example:**



Internet Early Warning System
→ Separation to other Systems

System / Characteristics	IDS	NWM-Tools	Firewall	HoneyPot	Sniffer	IAS
Function	Detection of signatures and attack patterns	Detection of Failures, configuration and performance Management, Accounting	Control of the communication by the means of rules and policies	Detection and Analyzing of the Intrusion and the used proceeding of hackers	Fault detection, spying on data and information	Actual status, pattern formation, creation of knowledge base, alarm signaling, forecasting
Location	Uplink	In the network	Uplink	Uplink	Uplink & Transit	Uplink & Transit
Realization	Complete analysis of the network traffic	Collection of Information by the means of agents	Complete analysis and control of the network traffic	Simulating the behavior of systems	Complete analysis of the network traffic	Complete analysis of the network traffic
Results	Recognition of signatures, Information for pattern formation	Accounting, fault messages, performance data	Security relevant information	Attack patterns and scenarios	Complete network traffic	Statistics, counters, results of further processing
Data privacy	Special agreement with concerned	Special agreement with concerned	Special agreement with concerned	Problem in specific scenarios	Very problematic	privacy compliant by design

Methods of realization
→ Existing systems

- Symantec DeepSight Threat Management System
- X-Force Threat Analysis Service von ISS
- Arbor Networks Peakflow X / SP
- Computer Associates – eTrust Network Forensics
- DShield.org – Distributed Intrusion Detection System
- **Internet Analysis System (IAS) of the Institute for Internet Security**
- **Internet Availability System (IVS) of the Institute for Internet Security**
- CarmentiS

Content

- Aim and outcomes of this lecture
- Motivation of
  Internet Early Warning System (IEWS)
- Targets of IEWS
- Structure of IEWS
- Process of IEWS
- Different realization of IEWS
- **Summary**

Summary
→ Internet Early Warning System (1/2)

- **Generation of an IT security situation awareness of the Internet (global view)**
  - **Current status**
    (Security, availability, Load, Spreading of protocols and services …)
  - **Existing attack scenarios**
    (Statistics on detected attacks …)
  - **Trends in general**
    (Technology, Protocols, Services …)
  - **Threat potential of the Internet**
    (Weakness, potential …)

- **The common global view helps:**
  - To judge the own local view more precisely.
  - React on developing trends very early to encounter potential damage in time.

Summary
→ Conclusion

- **Internet**
  - The internet is a critical infrastructure for our society
  - We need a trusted infrastructure to protect our future
  - Organisations running the infrastructure need to cooperate

- **We need the global view of the Internet**
  - To identify the current status
  - To see the new trends
  - To get ´early warnings´ to reduce damage
  - To make forecasts which help us to avoid damage

- Analogical to natural disaster warning systems, like the Tsunami warning system, we need a warning system for the internet to be able to issue counteractive measures before the actual threat strikes at us.

Fachhochschule Gelsenkirchen

Internet Early Warning System → Basis

Thank you for your attention!
Questions?

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Internet Early Warning System
→ Literature

- [1] Dr. Sabine Graumann and Florian Neinert. Monitoring Informationswirtschaft 9. Faktenbericht 2005, 2006.
- [2] BSI. Die Lage der IT-Sicherheit in Deutschland 2005. Technical Report, Bundesamt für Sicherheit in der Informationstechnik, 2005.
- [3] http://de.wikipedia.org
- [4] Stefan Korte: Internet-Frühwarnsysteme (internet early warning systems), Diploma Thesis, University of Applied Sciences Gelsenkirchen, 2006

Links:

Institute for Internet Security:
http://www.internet-sicherheit.de/forschung/aktuelle-projekte/internet-frhwarnsysteme/

SANS Internet Storm Center
http://isc.sans.org/