



Sicherheitsgruppe SGRP
Alumniorganisation Informatiksicherheit FHZ Luzern


Arbeitsgruppe "Monitoring & Incident Handling"

Erkenntnisse, Tipps & Tricks der Arbeitsgruppe
anlässlich der SGRP Frühjahrsveranstaltung 2003
in Luzern

www.sgrp.ch 26.05.2003 SGRP Frühjahrsveranstaltung 2003 1

Agenda

- Einführung
- Teil 1: Begriffsdefinitionen
"Monitoring & Incident Handling"
- Teil 2: Kritische Hinterfragung
 - Was bringt's...?
 - ... und was eben nicht?
- Teil 3: Praktische Tipps & Tricks
- Fragen & Antworten



www.sgrp.ch 26.05.2003 SGRP Frühjahrsveranstaltung 2003 2

Was ist die Motivation?

- Einführung

- Teil 1
- Teil 2
- Teil 3
- Q&A



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

3

Die Arbeitsgruppe

- Einführung

- Teil 1
- Teil 2
- Teil 3
- Q&A

- 14 Mitglieder diverser Firmen
- Start: 14. Oktober 2001
- 11 Sitzungen zu diversen Themen:
 - Begriffsdefinitionen
 - Monitoring
 - Incident Handling
 - Praktische Beispiele
 - Forensics
 - Return on Security Investment
 - IDS Produkte



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

4

Team Mitglieder

- Einführung
- Teil 1
- Teil 2
- Teil 3
- Q&A

- Titus Elsenberger:	UBS
- Daniel Eugster:	KPMG
- Gernot Franschitz:	Coutts Bank
- Tom Hager:	InfoTrust AG
- Andrea Klaes:	Swiss Re
- Peter Kunz:	DaimlerChrysler AG
- Virginia Maeder:	Swiss Re
- Karl Meier:	Kasec Engineering GmbH
- Roland Portmann:	HSW Luzern
- Thomas Risch:	UBS
- Heinz Schiffmann:	RTC
- Martin Sibler:	Swiss Re
- Frank Stäubli:	Swiss Re
- Anthony Thorn:	ATSS


www.sgrp.ch
26.05.2003
SGRP Frühjahrsveranstaltung 2003
3

Teil 1: Begriffsdefinitionen

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

"Monitoring & Incident Handling"






www.sgrp.ch
26.05.2003
SGRP Frühjahrsveranstaltung 2003
4

Definition Logging, Monitoring (1)

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Logging**
The process of **recording** events at the time that they occur.
- **Monitoring**
The **analysis, assessment, and review** of data collected for the purpose of controlling the system's **availability**.
- **Security Monitoring**
The **analysis, assessment, and review** of audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted **violations of system security**.



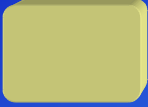

www.sgrp.ch


26.05.2003 SGRP Frühjahrsveranstaltung 2003 7

Definition Logging, Monitoring (2)

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Event**
A defined occurrence which could influence a system.
- **Security Event**
An event that is relevant to the security of the system.




www.sgrp.ch

26.05.2003 SGRP Frühjahrsveranstaltung 2003 8

Definition Logging, Monitoring (3)

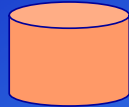
- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Logfile, Log**

The physical container of timestamped events.

- **Audit Trail**

A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.



Definition Logging, Monitoring (4)

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Investigation**

Collecting information from and about computer systems.

- **Forensics**

Collecting information from and about computer systems that is admissible in a court of law.

(The terms "investigation" and "forensics" are often used synonymously)



Definition Logging, Monitoring (5)

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

Event Detection
← triggering →

Event Recording
← logging →

Event Analysis
← monitoring →

Investigation

```

graph LR
    Cause[Cause] -- triggers --> Event[Event]
    Event -- logged to --> Log[(Log)]
    Log -- analyzed --> Results[expected results  
violation reports  
unexpected results to be investigated]
    
```

www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

11

Definition Incident Handling (ISO)

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Exploit**
"A defined way to breach the security of an IT system through a vulnerability."
- **Attack**
"An attempt to exploit an IT system vulnerability."
- **Intrusion**
"A deliberate or accidental set of events that potentially causes unauthorized access to, activity against, and/or activity in, an information technology (IT) system."

```

graph TD
    Exploit[Exploit] --> Attack[Attack]
    Attack --> Intrusion[Intrusion]
    Intrusion --> System[(System)]
    
```

www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

12

Beispiel anhand SQL Slammer

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Exploit**
SQL Slammer Wurm ist entwickelt
- **Attack**
SQL Slammer Wurm is "in the wild"
- **Intrusion**
SQL Slammer Wurm ist in System eingedrungen



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

13

Definition Incident Handling (CERT®/CC)

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Vulnerability**
"an aspect of a system or network that leaves it open to attack"
- **Threat**
"any circumstances or event that has the potential to cause harm to a system or network"
- **Incident**
"an instance of any computer security threat"



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

14


Beispiel anhand SQL Slammer

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A


- **Vulnerability**
 - Microsoft SQL Server, ungepatcht



- **Threat**
 - Port 1434/UDP offen gegenüber Internet
 - SQL Slammer Wurm



- **Incident**
 - Netzüberlastung durch sich verbreitenden SQL Slammer



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

13

Definition Incident Handling (CERT®/CC)

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Incident Handling**
Incident handling includes three functions: **Incident Reporting**, **Incident Analysis**, and **Incident Response**.
- **Incident Reporting**
 - serving as a central point of contact for reporting local problems.
- **Incident Analysis**
 - reviewing and correlating information to determine trends and patterns of intruder activity
 - taking an in-depth look at an incident report or incident activity to determine the scope, priority, and threat of the incident
 - researching possible response and mitigation strategies.
- **Incident Response**
 - sending out recommendations for recovery, containment, and prevention.
 - sharing information and lessons learned



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

14

Definition Incident Handling (CERT®/CC)

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **CSIRT**
 - A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity.
- **CIRC, CIRT, IRC, IRT, SERT, SIRT**
 - Acronyms for incident response teams
- **CERT, CERT/CC**
 - "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office
- **CERT/CC**
 - The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.
- **FIRST**
 - Forum of Incident Response Teams



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

17

Definition Incident Handling (CVE)

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A


- **Universal Vulnerability**

A universal vulnerability is a state in a computing system (or set of systems) which either:

 - allows an attacker to **execute commands** as another user
 - allows an attacker to **access data** that is contrary to the specified access restrictions for that data
 - allows an attacker to **pose as another entity**
 - allows an attacker to **conduct a denial of service**
- **Exposure**

An exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either:


 - allows an attacker to conduct **information gathering** activities
 - allows an attacker to **hide activities**
 - includes a capability that behaves as expected, but **can be easily compromised**
 - is a **primary point of entry** that an attacker may attempt to use to gain access to the system or data
 - is considered a problem according to some reasonable security policy



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003




18

Definition Intrusion Detection

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Intrusions**
Attacks from outside the organization
- **Misuse**
Attacks from within the organization
- **Intrusion Detection System (IDS)**
An intrusion detection system gathers and analyzes information from various areas to identify possible security breaches, which include both intrusions and misuse.
- **Network IDS (NIDS)**
Gathers information from the network.
- **Host IDS (HIDS)**
Gathers information from the host itself.



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

19

Quellenangaben

- Einführung
- **Teil 1**
- Teil 2
- Teil 3
- Q&A

- **Logging / Monitoring**
eigene Begriffsdefinitionen, basierend auf allgemeinen Security Glossaries, z.B.:
- http://www.isse.gmu.edu/~csis/glossary/merged_glossary.html
- <http://www.setsolutions.com/security.htm>
- <http://sun.soci.niu.edu/~rslade/secgloss.htm>
- <http://www.ietf.org/rfc/rfc2828.txt>
- <http://www.yourwindow.to/information-security/>
- **CVE Definitionen**
<http://www.cve.mitre.org/about/terminology.html>
- **CERT/CC Definitionen**
<http://www.cert.dfn.de/eng/pre99papers/certterm.html>
http://www.cert.org/csirts/csirt_faq.html
- **ISO Definitionen**
SC 27 Standing Document 6 (SD 6),
Glossary of IT Security Terminology (SC 27 N 2776)



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

20

Teil 2: Kritische Hinterfragung

- Einführung
- Teil 1
- **Teil 2**
- Teil 3
- Q&A

- Was bringt's ...?
- ... und was eben nicht?



SGRP
www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

31

Gründe für Security Monitoring

- Einführung
- Teil 1
- **Teil 2**
- Teil 3
- Q&A

- Prävention allein genügt nicht
 - Es gibt immer neue Angriffsarten, welche man nicht verhindern, sondern nur erkennen kann.
→ Detection
- Monitoring als Grundlage für Detection & Investigation
- Zusatznutzen:
 - Misconfiguration Detection
 - Trends & Statistics
 - Response

SGRP
www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

32

Falsche Erwartungen

- Einführung
- Teil 1
- **Teil 2**
- Teil 3
- Q&A

- Es gibt eine einheitliche Definition der Begriffe
- IDS erkennt alles
- IDS läuft automatisch, ohne Fachpersonal
- IDS kostet nichts
- IDS ist genormt, kompatibel und skalierbar
- IDS reduziert Risiken
- IDS verhindert jede Art von Missbrauch
- Technische Massnahmen genügen



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

23

Voraussetzungen

- Einführung
- Teil 1
- **Teil 2**
- Teil 3
- Q&A

- Kritische Bereiche identifizieren (Analyse)
- Organisation & Prozess definieren
 - Eskalation & Response
 - Unterhalt des Systems
 - Monitoring – Wer schaut die Logs an und wertet sie aus?
- Genügend Ressourcen müssen vorhanden sein
 - Zeit, Geld, Personal (inkl. Know-How)
- Inventar der gesamten Infrastruktur
 - Systeme (Server, Client, Router, ...)
 - Netzwerkverbindungen
 - Anwendungen, Services



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

24

Erfahrungsaustausch

- Einführung
- Teil 1
- **Teil 2**
- Teil 3
- Q&A

The illustration shows a group of people sitting around a table in a meeting room. Five thought bubbles are connected to the scene, each containing a different icon: a thief with a bag, a stack of money, a hard drive, a scale of justice, and a calculator with a ruler and the word 'PLANS'.

SGRP
www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

33

Schlussfolgerungen zum Thema IDS (1)

- Einführung
- Teil 1
- **Teil 2**
- Teil 3
- Q&A

- Tools sind nur ein Teil des Projektes, aber ein wichtiger
- Das organisatorische Umfeld muss definiert sein
- Notfallabläufe müssen vom Topmanagement verabschiedet sein
- Fachkenntnis vor allem notwendig für eine zeitgerechte Implementierung
- Kein Wundermittel gegen alles Böse
- Sehr Ressourcenintensiv (Geld und Personal)

SGRP
www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003


34

Schlussfolgerungen zum Thema IDS (2)

- Einführung
- Teil 1
- **Teil 2**
- Teil 3
- Q&A

- ROSI sehr schwer nachweisbar (ROSI: **R**eturn **O**n **S**ecurity **I**nvestment)
- Modewort; Jeder spricht davon, doch keiner hat eine vollständige Lösung implementiert.
- Zusatznutzen ist erreicht, Hauptnutzen noch nicht

- **Die Zeit für ein IDS ist eher noch nicht da...**



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

27

Vorteile eines Intrusion Detection Systems

- Einführung
- Teil 1
- **Teil 2**
- Teil 3
- Q&A

- Events werden erkannt
 - Auch Events, welche vom Viren Scanner nicht erkannt werden, z.B. Root Kits
- Erkennen von Miskonfigurationen
- Erhöhung der Security Awareness
 - Änderung der "Patch-Kultur"
 - Fachwissen der IT Administratoren erhöht sich
- Untersuchen von Vorfällen wird möglich



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

28

Ausblick...

- Einführung
- Teil 1
- **Teil 2**
- Teil 3
- Q&A

- IDS ist integraler Bestandteil jedes Systems (Hardware oder Software)
- Selbstlernende IDS
- Marketing Angaben und Realität decken sich



www.sgrp.ch


26.05.2003 SGRP Frühjahrsveranstaltung 2003 29

Teil 3: Praktische Tipps & Tricks

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- Auf was muss man achten?





www.sgrp.ch

26.05.2003 SGRP Frühjahrsveranstaltung 2003 30

Objectives

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- What are you trying to achieve?
 - Incident Response
 - Additional layer of defence
 - Logging & Forensics
 - Patching problem



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

31

Objective Incident Response

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- Incident response - the appropriate reaction to the detection of an incident, is mainly an organisational issue as opposed to technical.
- A timely, effective incident response requires 7x24 staffing by technically qualified personnel and also 7x24 availability of decision makers.
- Are you prepared to pay for this?



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

32

Objective Additional layer of defence

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- Intrusion Detection Systems (IDS) are often described as providing an additional layer of defence.
- However you should be under no illusion that an IDS even implemented without budget restraints will detect ALL intrusions. i.e. will be 100% effective.



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

33

Objective Logging & Forensics

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- In certain circumstances effective logging may be the principal objective. This is advantageous because it supports such difficult areas as incident response, inventory.
- If the logging is intended to be usable in a court of law (implied by the term forensics) the task becomes significantly more difficult.
- Logging is a prerequisite for forensics.



www.sgrp.ch


26.05.2003

SGRP Frühjahrsveranstaltung 2003

34

Objective Patching problem (1)

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

33

- Most of us agree that we would prefer to prevent an intrusion as opposed to responding to one.
- However nowadays we are obliged to live with buggy software, newly discovered vulnerabilities and frequent patches.
- The delay between discovery of a vulnerability and deployment of the patch is the "Window of vulnerability", and if the patch is to be staged and tested this window is lengthy.

Objective Patching problem (2)

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A




www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

35



Vulnerability Discovered **Vulnerability Published** **Patch Available** **Decision to Patch** **Test Patch** **Deploy Patch**

Using a signature based IDS it should be possible to shorten the window of vulnerability. The effectiveness of this approach depends on the quality of the Incident Response process.



Vulnerability Discovered **Vulnerability Published** **Signature Available & Deployed** **Decision to Patch** **Test Patch** **Deploy Patch**

Location of Sensors (1)

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

■ Network based:

- Network sensors rely on recognising signatures and simple sequences thereof, and are less appropriate when non-standard components or architectures are used. The positioning of the sensors in the network depends on the objectives, but a good starting point is behind the Internet firewall.
- Network sensors are bad at detecting internal attacks, and useless against attacks whose signatures are not known (analogy to virus scanners). The vendors provide regular signature updates.



www.sgrp.ch

26.05.2003

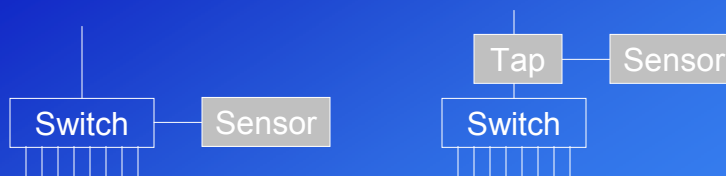
SGRP Frühjahrsveranstaltung 2003

37

Location of Sensors (2)

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- Network Sensors can tap the network or not.



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

38

Location of Sensors (3)

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

■ Host based

- IDS will generally include integrity checking of critical files and analysing logs for predefined events and sequences of events.
- This makes host based IDS potentially more powerful, but more difficult to deploy and use.



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

39

Type of Sensor

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

■ There are 3 main approaches:

- **Integrity checking.** Files which should not change are checked at regular intervals against a cryptographic checksum. This can potentially detect unknown attacks.
- **Knowledge based.** This involves looking for attack signatures and therefore cannot detect an unknown attack, but it is easier to update signatures than to patch a system.
- **Behaviour based.** Artificial Intelligence or statistical systems which look for unusual behaviour by learning „normal behaviour“ are (mostly) still in the laboratory.



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

40

Correlation & Analysis

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- Correlation involves combining the output of various sensors in order to be able to identify and classify/prioritise an attack.
- Both Network and Host-Based IDS vendors provide correlation functionality.
- Systems to combine the output of Network sensors with Host-based systems are not yet available.
- Specialised Security Management vendors offer proprietary correlation and analysis tools for other vendors sensors.



26.05.2003

SGRP Frühjahrsveranstaltung 2003

41

High speed networks

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- Today's network sensors cannot handle heavily loaded high speed networks.



26.05.2003


SGRP Frühjahrsveranstaltung 2003

42

Automated Response

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- If we are going to rely on your IDS to prevent attacks, it is not enough to detect attack signatures.
- The real and critical attack must be quickly distinguished from all the false alarms, and an appropriate response implemented very rapidly.
- An automated response (e.g. blocking certain source addresses) appears to be an attractive approach, but is vulnerable to denial of service. Active automated response (attacking the attacker) is generally considered unacceptable.
- Nonetheless, IPS is the new "Buzzword"!



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

43

Inventory!

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- An "out-of-the box" IDS will generate thousands of false alarms.
→ Obviously the signature of a Windows vulnerability is not relevant to a Unix system.
- The real problem is more complicated and requires detailed information about the systems to be protected (Inventory) - e.g. type of software deployed with patch level - so that the significance of each event can be evaluated.



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

44

Outsourcing (1)

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- The Security Management sector is expected to show phenomenal growth over the next few years. The correlation (normalisation) and analysis of sensor output can arguably be outsourced more efficiently than performed in house.
- You will know the true cost!
- Your managed security vendor should provide a SLA which specifies (among other things) response times for various levels of alert.



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

43

Outsourcing (2)

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- Alerts must be prioritised, eg.
 - Level 0 Insufficient information (inventory?)
 - Level 1 Possible attack to which customer is vulnerable
 - Level 2 Possible attack customer is not vulnerable
 - Level 3 etc.
- However (unless you outsource the response – which is not usual) your organisation will still have to make staff available 7x24 who are capable of making important decisions quickly.



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

44

Tuning

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- Tuning, Normalisation: As described above an out of the box IDS will generate thousands of false alarms. The tuning process must reduce this to a handful of "serious" alerts which then have to be analysed manually. This tuning process can be expected to take a few months.
- It would be naive to imagine that the tuning process will be perfect. It involves a tradeoff of False alarms against Missed intrusions (viz. Biometrics).



www.sgrp.ch

26.05.2003


SGRP Frühjahrsveranstaltung 2003

47

Summary

- Einführung
- Teil 1
- Teil 2
- **Teil 3**
- Q&A

- **Buying an IDS is only a small part of an effective defence.** Inventory, Tuning and Incident Response processes are major items.
- Doing it properly will be very expensive!
- An IDS with an effective incident response team does not replace properly configured firewalls, hardened servers, etc.
- Even a well deployed IDS will not detect (never mind prevent) 100% of attacks.
- **This does not mean you should forget it!**



www.sgrp.ch

26.05.2003

SGRP Frühjahrsveranstaltung 2003

48

Fragen & Antworten

- Einführung
- Teil 1
- Teil 2
- Teil 3
- **Q&A**

■ Was ist nun noch unklar?

