GI Fachgruppe SIDAR

FG-Sitzung

24. November 2003

Themen der Fachgruppen-Sitzung

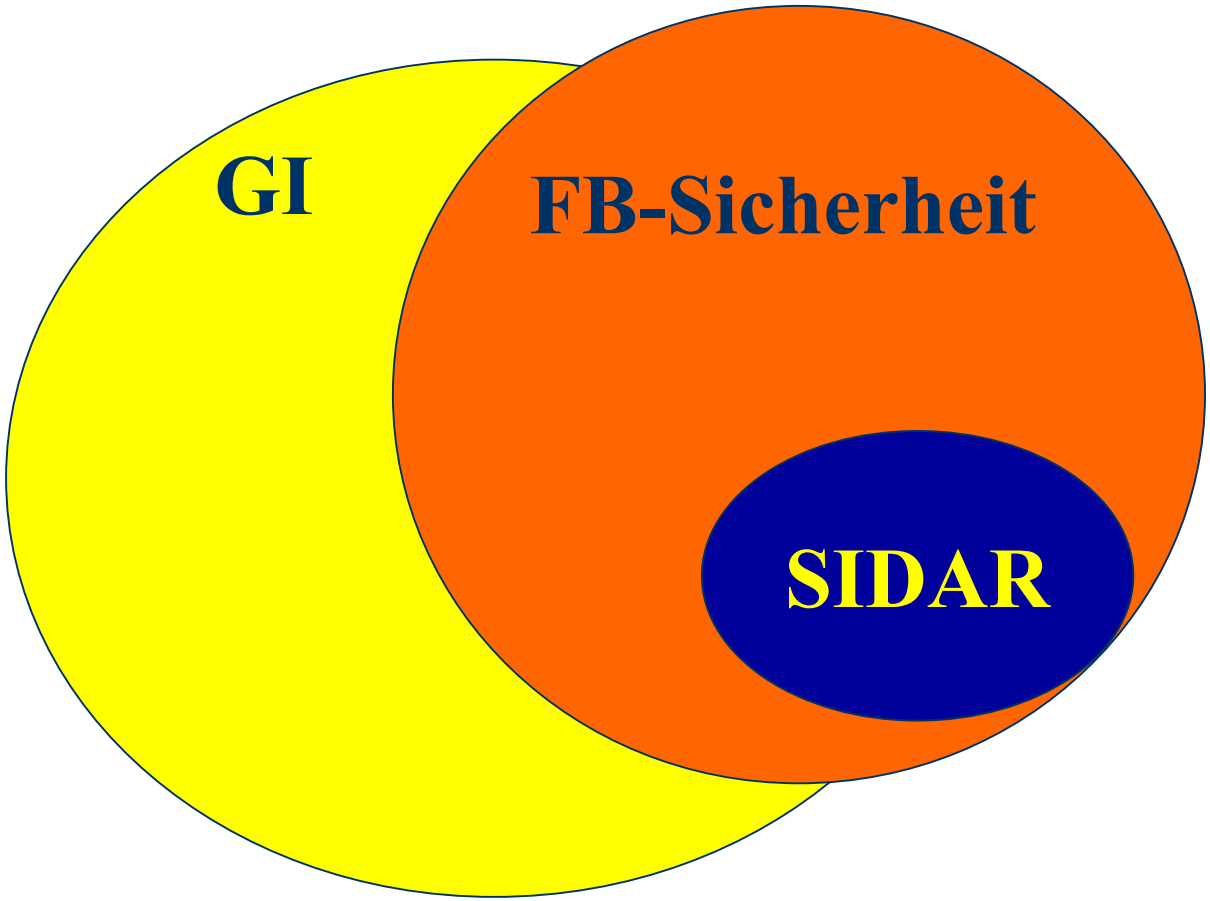
- Kurze Vorstellung der Fachgruppe
  - Gegenstand und Ziele der Fachgruppe
  - Leitungsgremiums
- Aktivitäten
  - Erfahrungen mit bisherigen Aktivitäten
  - Zusammenfassende Bewertung
- Planung zukünftiger Aktivitäten
  - DIMVA 2004
  - Ideen für neue Aktivitäten
- Organisatorische Frage
  - Mitgliederwerbung
  - Vorbereitung der Wahlen zum Leitungsgremium

Was ist SIDAR?

- Deutsch:
  - Erkennung und Beherrschung von Vorfällen der Informationssicherheit
- Englisch:
  - Security - Intrusion Detection and Response

- ... Eine Fachgruppe innerhalb des Fachbereichs Sicherheit innerhalb des GI e. V.

Ein Bild sagt mehr als ...



Erkennung und Beherrschung von Vorfällen der Informationssicherheit

- Häufige Angriffe auf und Vorfälle bei IT-Systeme
  - Hohe direkte Schäden
  - Nicht abzuwägende Folgeschäden
- Mangelnde Vorbereitung
  - Ohne direkte Schäden (oft) keine Erkennung
  - Keine Verfahren für eine angemessene Reaktion
- Fehlerhafte oder fehlende Sicherheitskonzepte bei Protokollen, Anwendungen und Betriebssystemen
  - Neue Sicherheitslücken haben weltweite Implikationen
  - Im Wettlauf gegen die Zeit sind Lücken zu schließen

Erkennung und Beherrschung von Vorfällen der Informationssicherheit

- Unternehmensweite Verfahren und übergreifende Kooperationen sind der Schlüssel für eine erfolgreiche Erkennung bzw. Beherrschung
- Themengebiete:
  - Warnungen und Alarmierungen (Sicherheitslücken, etc.)
  - Erkennung (Anti-Viren, Intrusion Detection)
  - Notfallvorsorge, Betreuung bei Vorfällen (CERT, Incident Response Teams, Sicherheitsteams)
  - Aufklärung und Analyse (Digitale Forensik)
  - Wechselwirkungen mit präventiven Maßnahmen
  - Anpassungs- / Verbesserungsmöglichkeiten aus der Praxis

Zielgruppen
- Wer soll angesprochen werden?

- Angesprochen als Mitglieder:
  - Fachleute
  - Wissenschaftler
  - Entscheider
- Außenwirkung auf:
  - Informatiker und Entscheider (vorrangig)
  - Weitere Entscheidungsträger

Vision der Fachgruppe
- Wie soll es in Zukunft aussehen?

- Es gibt geeignete und nutzbaren Methoden und Verfahren zur Erkennung und Beherrschung von Vorfällen der Informationssicherheit.
- Der Nutzen dieser Methoden und Verfahren ist allgemein bekannt. Methoden und Verfahren werden von Anwendern und Verantwortlichen akzeptiert.
- Der breite Einsatz dieser Methoden und Verfahren erfolgt im Rahmen wirtschaftlicher und gesellschaftlicher Abwägungen.
- Bislang getrennt betrachtete Aspekte wie reaktive, präventive und organisatorische Methoden und Verfahren wirken integriert zusammen.

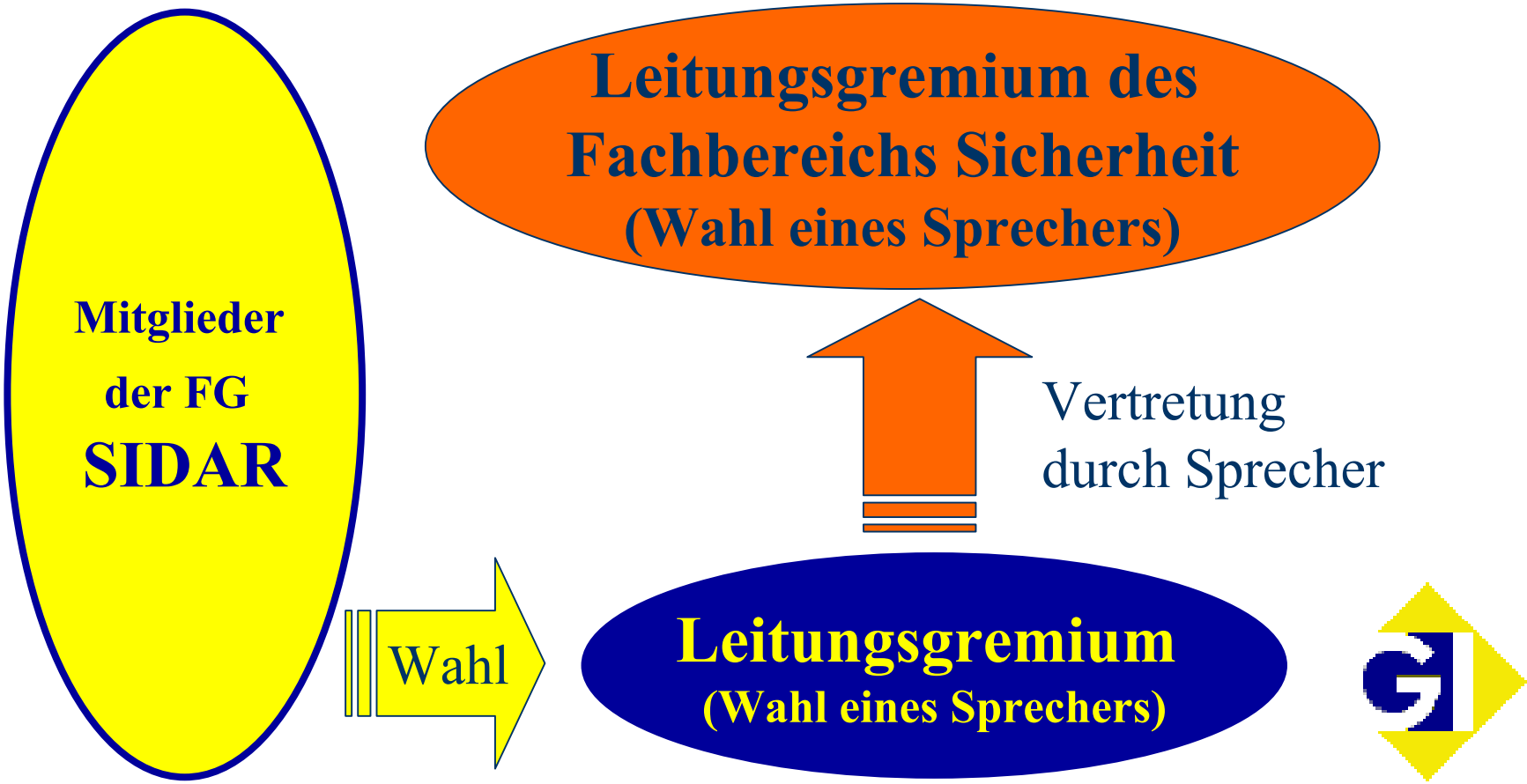
Mission der Fachgruppe - Was muss dazu geschehen?

- Neutraler Ansprechpartner für die Fachleute und Wissenschaftler, die die Entwicklung geeigneter Methoden und Verfahren vorantreiben.
- Förderung eines fachlich integrierenden Austausches über präventive, reaktive und organisatorische Methoden und Verfahren auf nationaler und internationaler Ebene.
- Verbreitung des Wissens über Methoden und Verfahren sowie die Schaffung eines entsprechenden Bewusstseins für deren Vorteile, Nutzen und Wirtschaftlichkeit.
- Förderung und Mitgestaltung der Entwicklung von Methoden und Verfahren.

Leitungsgremium

- Ulrich Flegel (stv. Sprecher)
- Klaus-Peter Kossakowski (Sprecher)
- Michael Meier
- Jens Nedon
- Markus Nolte
- Andreas Prass

Ein Bild sagt mehr als ...



Aktivitäten

- Fachliches Engagement
  - DFN-CERT Workshop 2003
  - CTOSE 2003
- Erfahrungen mit bisherigen Aktivitäten
  - IMF 2003

Bewertung der Aktivitäten

- Auf Veranstaltungen konzentriert
- Mit IMF 2003 und Planungen für DIMVA 2004 erste eigene Gehversuche
- Problem, wie so oft bei ähnlichen Aktivitäten:

➔ **Freiwilliges Engagement!**

Planung zukünftiger Aktivitäten

- DIMVA 2004
- Web-Auftritt
  - Logo
  - Inhalte
- Ideen für neue Aktivitäten

Organisatorische Frage

- Mitgliederwerbung
- Vorbereitung der Wahlen zum Leitungsgremium

Wahlen zum Leitungsgremium (1)

- Verabschiedung der FG-Ordnung
- Festlegung
  - Wahltermin ➔ DIMVA 2004
  - Anzahl der Mitglieder ➔ 7 [Minimum ist 5]
  - GI-Mitgliedschaft der Kandidaten ist Pflicht
- Schriftliche Einladung 6 Wochen vor der Wahl
  - Anzahl der Kandidaten
  - Vorläufige Kandidatenliste

Wahlen zum Leitungsgremium (2)

- Eröffnung durch FB-Sprecher
- Wahlberechtigt sind nur Mitglieder der Fachgruppe
  - ➔ Nicht Mitarbeit zählt, sondern formale Anmeldung bei GI
- Wahl eines Wahlleiters und zweier Auszähler
- Frage nach weiteren Kandidaten
- Alle Kandidaten müssen schriftlich / mündlich vorher ihre Zusage geben, zur Verfügung zu stehen
- Gewählt sind Kandidaten mit positiver Stimmenbilanz und größter Differenz zwischen „Ja“ und „Nein“
- Geheime, schriftliche Wahl

... noch Fragen?
... mehr Diskussion?

Gerne ;)