

GI Fachgruppe SIDAR

FG-Sitzung
6. Juli 2004



Themen der Fachgruppen-Sitzung

- Kurze Vorstellung der Fachgruppe
 - Gegenstand und Ziele der Fachgruppe
- Wahlversammlung
 - Vorstellung der Kandidaten
 - Durchführung der Wahlen zum Leitungsgremium
- Aktivitäten
 - Erfahrungen mit bisherigen Aktivitäten
 - Zusammenfassende Bewertung
- Planung zukünftiger Aktivitäten
 - PRIMA 2005
 - Sicherheit 2005
 - Ideen für neue Aktivitäten

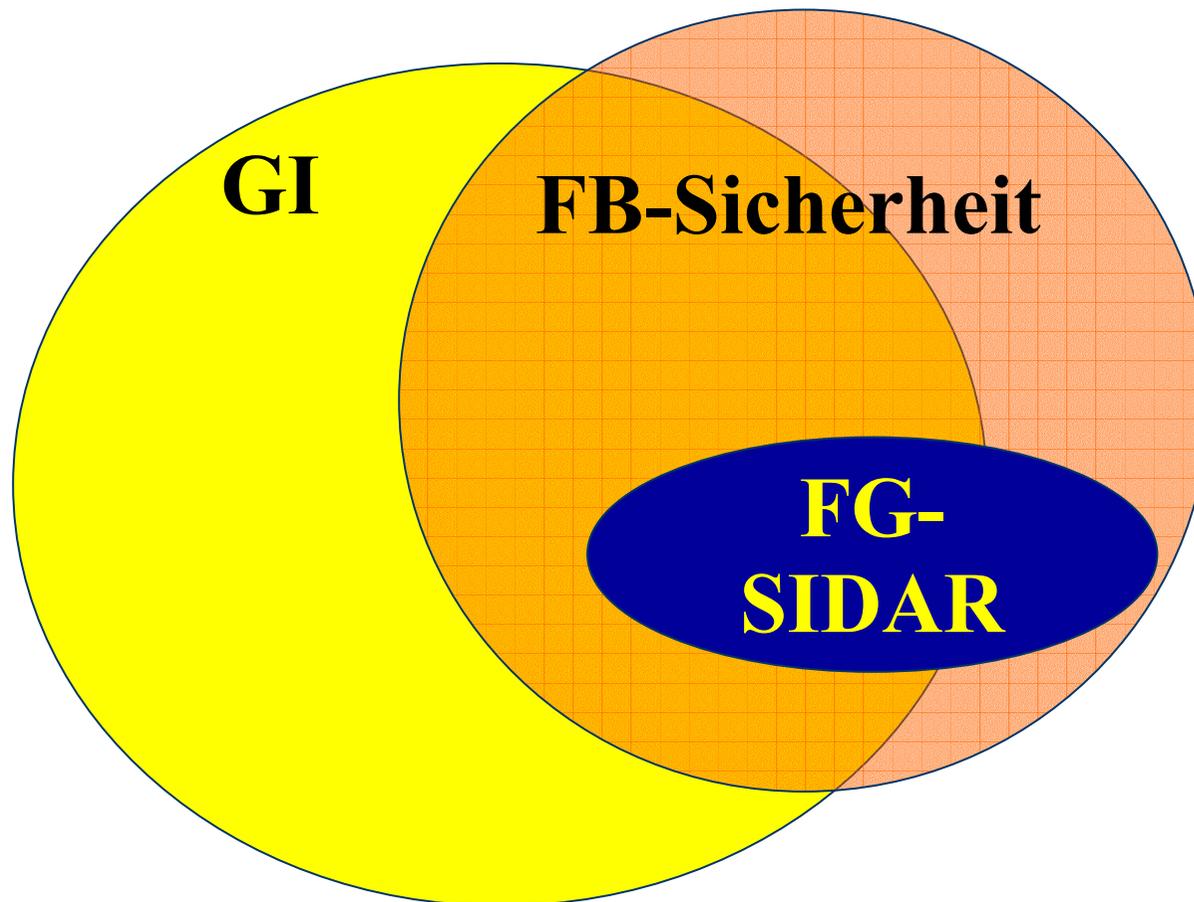


Was ist SIDAR?

- 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 nutzbare 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.
- Bisherig getrennt betrachtete Aspekte wie reaktive, präventive und organisatorische Methoden und Verfahren wirken integriert zusammen.



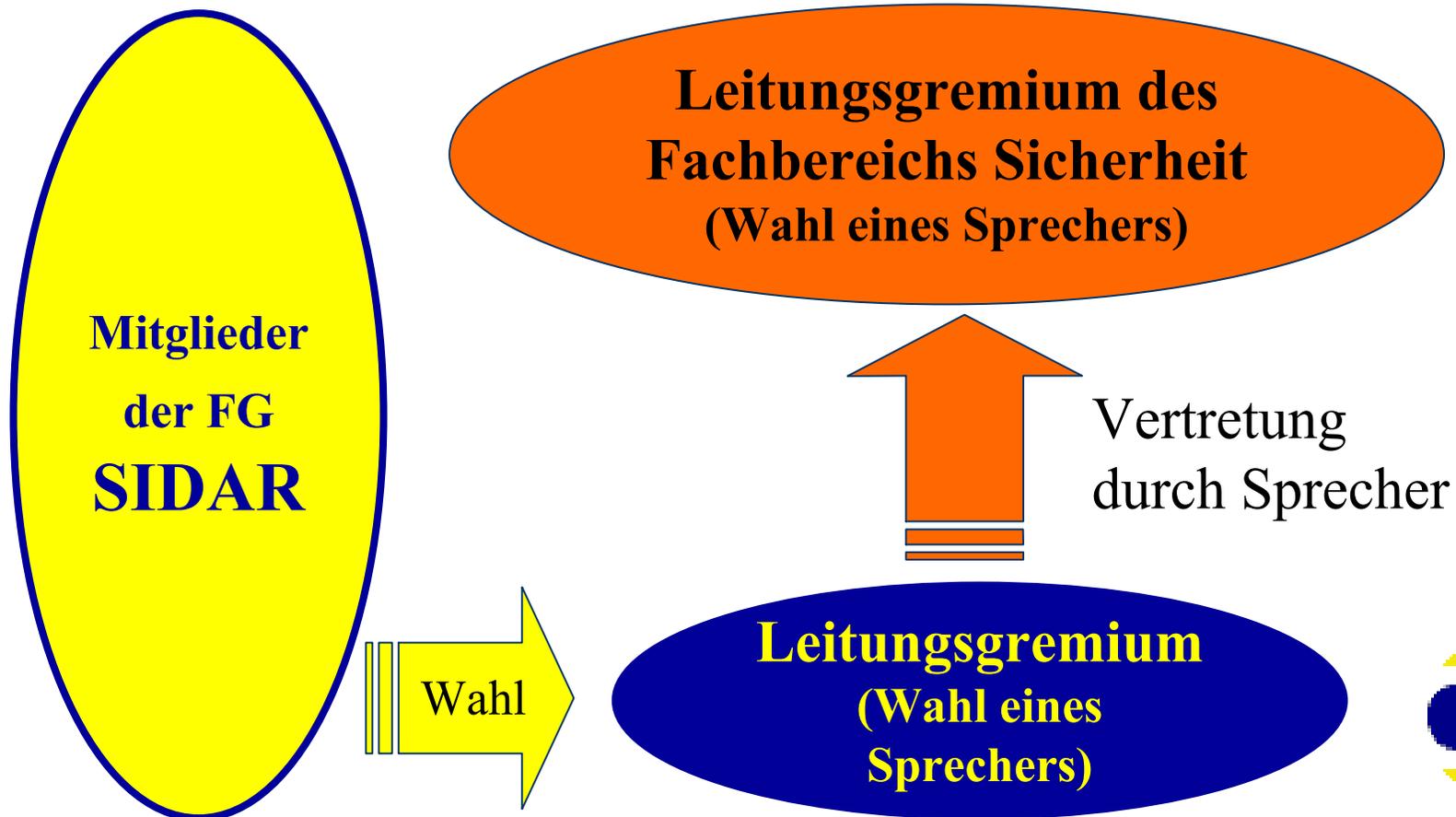
Mission der Fachgruppe

- 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.



Ein Bild sagt mehr als ...



Bisheriges Leitungsgremium

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



Gewähltes Leitungsgremium

- Roland Büschkes (T-Mobile)
- Ulrich Flegel (Univ. Dortmund)
- Oliver Göbel (Univ. Stuttgart)
- Detlef Günter (Volkswagen)
- Oliver Heinz (Arago)
- Marc Heuse (n.runs)
- Michael Meier (TU Cottbus)
- Werner Metterhausen (VZM)
- Jens Nedon (Consecur)
- Dirk Schadt (CA)



Aktivitäten

- Fachliche Beteiligung
 - DFN-CERT Workshop 2003 und 2004
 - CTOSE 2003
- Eigene Veranstaltungen
 - IMF 2003
 - DIMVA 2004



Bewertung der Aktivitäten

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

→ Freiwilliges Engagement!



Planung zukünftiger Aktivitäten

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



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

Gerne ;)

