
IT-Frühwarnsysteme in Deutschland

Workshop von BITKOM und BMWA

IT-Frühwarnsysteme in der ITK-Industrie

Berlin, 2004-05-13

Paul Frießem, Fraunhofer SIT

paul.friessem@sit.fraunhofer.de

www.sit.fraunhofer.de

Überblick

1. Anforderungen an Frühwarnsysteme
2. FWS in der ITK-Industrie:
Nutzung, Erwartungen, Einschätzungen
3. FWS in der ITK-Industrie: Wo liegen die Probleme?
4. FWS in der ITK-Industrie: ein denkbares SOLL
5. Beispiele aus verwandten Bereichen
6. Offene Fragen

Anforderungen an Frühwarnsysteme

- Noch **unbekannte Schwachstellen** erkennen / erahnen
 - **Geplante / eingeleitete Angriffe** auf IT-Infrastrukturen rechtzeitig erkennen (Ziele und Methoden)
 - Auf erkannte / verifizierte Schwachstellen wirksam reagieren
 - Auf geplante / eingeleitete Angriffe wirksam reagieren
- **Critical Infrastructure Protection (CIP)**

FWS in der ITK-Industrie: Der Hintergrund



- EU-Roadmap-Projekt **ACIP** in 2002 – 2003
 - Analysis & Assessment for CIP
 - Gefördert durch EC: IST-2001-37257
 - www.acip-eu.de
- Ermittlung der **TK-Betreibersicht** hinsichtlich:
 - Bedrohungen und Risiken für kritische Prozesse
 - Gegenwärtig eingesetzte CIP Methoden und Maßnahmen
 - Anforderungen und Erwartungen an CIP Methoden / Werkzeuge

FWS in der ITK-Industrie: Was wird genutzt?

- Hauptmethode für Bewertungen und Gegenmaßnahmen: **Leitstände** und **Menschliche Expertise**; „**Best practice**“ allgemein akzeptiert
- **Informationsaustausch** (offiziell und inoffiziell) gut etabliert
- **Werkzeuge** auf einem eher niedrigen Level (etwa intrusion detection, security-scanner, log file analyser) und mit nicht immer befriedigenden Ergebnissen
- Kaum **Decision support** Systeme im Einsatz

FWS in der ITK-Industrie: Die Erwartungen

- **Bessere Trefferrate** bei Werkzeugen für Logging, Monitoring und intrusion detection
- Gemeinsames „**Datenaustausch-Protokoll**“ zum Sammeln von Basisdaten
- Geringe **Daten-Intensität** (für Input und Output)
- Vorhersagbare **Qualität** und **Vollständigkeit** der Ergebnisse
- **Verständlichkeit** und **Handhabbarkeit**

FWS in der ITK-Industrie: Einige kritische Einschätzungen

- **Decision support** Systeme
 - Eher geringes Vertrauen in Wissensmanagement- und Entscheidungsunterstützungs-Werkzeuge
 - Aufwand für Input-Daten, die laufende Aktualisierung der Basisinformationen und das Training der Benutzer zu hoch

- **Modellierungs-** und **Simulationswerkzeuge**
 - Zu hoher Aufwand für eine realitätsnahe Gestaltung

FWS in der ITK-Industrie: Wo liegen die Probleme?

- Die Probleme sind **global** und breiten sich **schnell** aus; die Lösungen sind leider oft nur **lokal** und **zeitaufwändig** zu aktivieren.
- Die **Fehlerhäufigkeit** in Software-basierten Systemen ist **hoch**, und die Fehler sind immer **neu**.
- Intuitiv gibt es **Bedenken**, zur Bekämpfung der Probleme wiederum **Software-basierte** Systeme einzusetzen.
- **Menschen** werden zum **schwächsten Glied** in der Frühwarnkette.

FWS in der ITK-Industrie: Ein denkbares SOLL

- Laufende **automatische Analyse** des Netz-/Systemverhaltens, um „Auffälligkeiten“ festzustellen
- **Selbstlernende Algorithmen**, um „gutwillige“ von „böswilligen“ Auffälligkeiten zu unterscheiden
- Regelbasiertes Ergreifen **automatischer Abschottungsmaßnahmen** gegen böswillige Auffälligkeiten
- Einschaltung von **Menschen** zur Detailanalyse und Steuerung weiterer Gegenmaßnahmen bzw. der Recovery



Beispiele aus verwandten Bereichen

- Das "**Global Early Warning Information System**"
GEWIS des NCS (National Communications System),
jetzt Teil des US Homeland Security Departments;
Endversion für 2004 angekündigt.
- Online-Analyse von **Kreditkartenzahlungen**:
"Visa Intelligent Scoring of Risk" (VISOR)
- Frühwarnsysteme für **ökonomische Risiken** von
Unternehmen (KonTraG, Basel II)
- **Data Mining, Artificial Intelligence, neuronale Netze**

Einige offene Fragen

- Kann das Problem erfolgreich auf **nationaler** Ebene angegangen werden?
- Ist der Ansatz zur **automatischen** Analyse und Einleitung von Gegenmaßnahmen wirklich tragfähig, oder erzeugt er nur **neue Schwachstellen**?
- Wie kann sichergestellt werden, dass Frühwarnungen **schneller** übermittelt werden als das Problem, vor dem sie warnen?
- Dient „Frühwarnung“ nicht nur zum Bekämpfen von **Symptomen**, wobei die **Ursachen ignoriert** werden?

IT-Frühwarnsysteme in Deutschland

Workshop von BITKOM und BMWA

IT-Frühwarnsysteme in der ITK-Industrie

Berlin, 2004-05-13

Paul Frießem, Fraunhofer SIT

paul.friessem@sit.fraunhofer.de

www.sit.fraunhofer.de