GI SIDAR SPRING 2006

Ein Sicherheitsportal zur Selbstverwaltung und automatischen Verarbeitung von Sicherheitsvorfällen als Schlüseltechnologie gegen Masseninfektionen

Jochen Kaiser, Alexander Vitzthum, Peter Holleczek,
Regionales Rechenzentrum
Falko Dressler
Lehrstuhl für Kommunikationssysteme
Universität Erlangen-Nürnberg

Motivation/
Probleme von Sicherheitsteams

- Mehr Sicherheitsvorfälle bedeuten mehr Arbeit für CSIRT Teams
- Masseninfektionen mit Malware erhöhen den „Geräuschpegel“ im Netzwerk
- Extrusion Detection wird aufwendiger
- Mehr Meldungen von externen CSIRTs über infizierte Systeme des lokalen Netzwerks.

→ Verringerung des „Geräuschpegels“ in den IT-Sicherheitsvorfällen

→ Unterscheidung zwischen **qualifizierten** und **unqualifizierten** IT-Sicherheitsvorfällen

Einsatz von Helpdesksystemen für CSIRT-Aufgaben

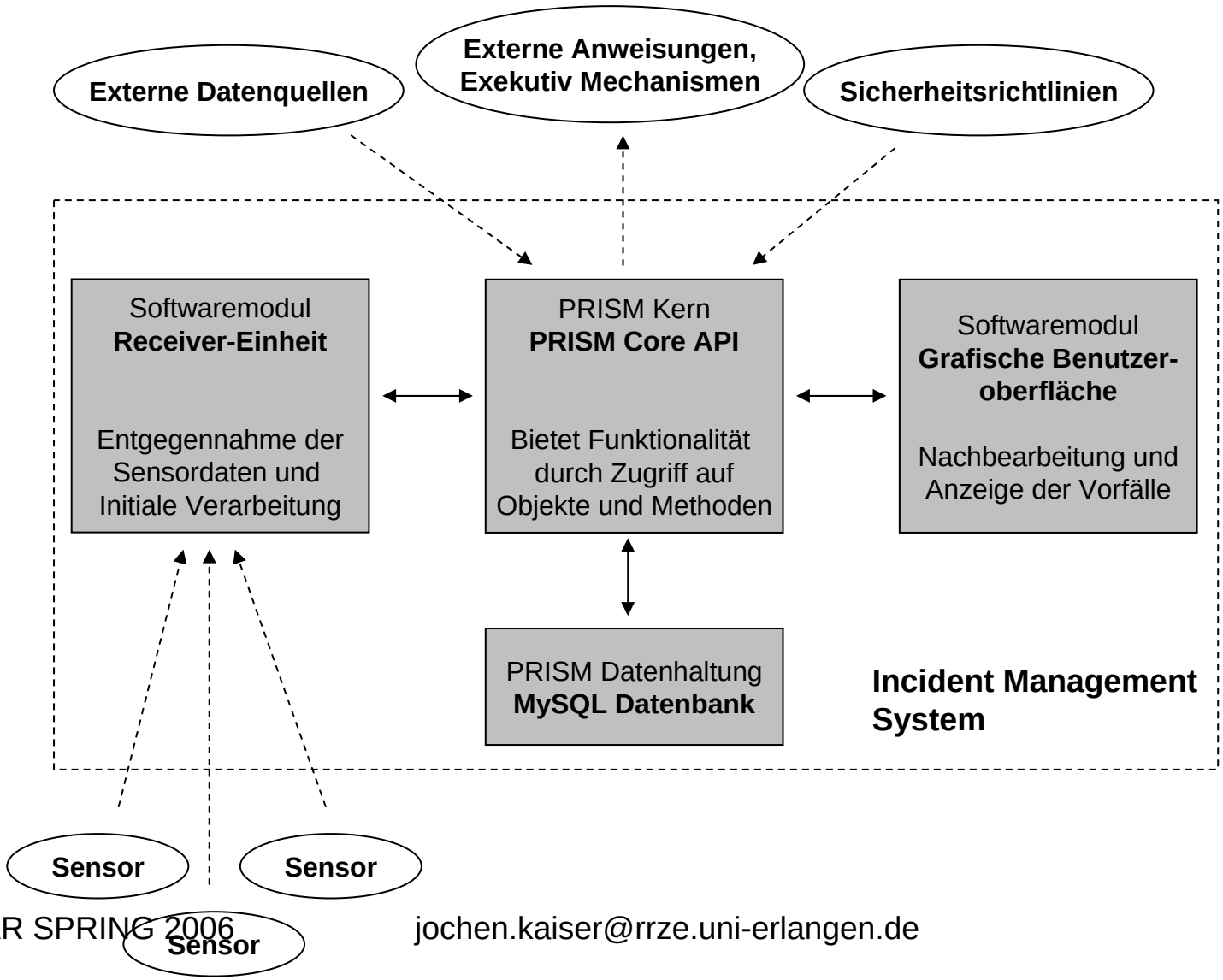
- Üblicherweise wird von CSIRTs ein modifiziertes Helpdesksystem eingesetzt. Bestandteile:
  - Mail2TT-Gateway
  - Warteschlangen mit der Möglichkeit zu Prioritisieren
  - Abfrageterminal über den Status des TT
  - Lösungsdatenbank
- Es fehlt:
  - Selbstauskunftsterminal mit vollem Funktionsumfang.
  - Automatische Kopplung von Sicherheitsvorfällen
  - Delegation der Vorfälle

→ **Entwicklung des Werkzeugs PRISM**
(Portal for Reporting Incidents and Solution Management)

Aufbau und Funktionsweise von PRISM

- Modulares System
- Komponenten: FreeBSD, Apache, MySQL, PERL
- Administrationsterminal
- Selbstauskunftterminal für Nutzer
- Eskalationsszenario
- Rollenmodell
- Unterstützung in der Lösungsfindung

Modularer Aufbau



Nebenbedingungen für den Einsatz der PRISM Architektur

- **Update-Netzwerke**
  Eine Menge von Systemen, welche Softwareaktualisierungen für die eingesetzten Netzwerke bereitstellen.

- **Sperrwerkzeug für einzelne Hosts**
  Ein Werkzeug muss die folgende Semantik verstehen:
  sperre <IP>
  entsperre <IP>
  Trotz Sperre müssen dennoch die Update-Netzwerke erreichbar sein!

- **Auskunftswerkzeug über die administrative Struktur**
  Ein System, welches als Eingabe die IP-Adresse eines Systems bekommt und als Ausgabe die Verantwortung für das System nennt.

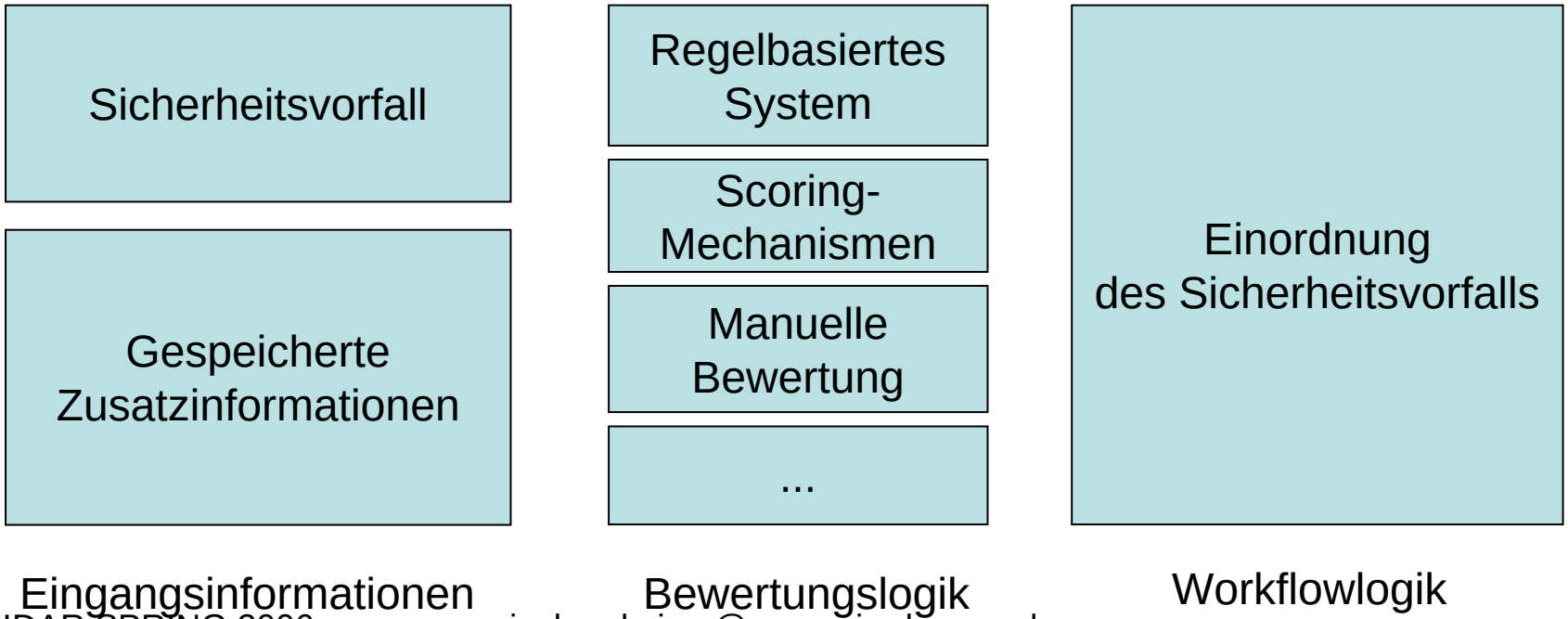
- **Option**: ***Werkzeug zum Umlenken von WWW-Anfragen*** im Netzwerk
  Die WWW-Anfragen des betroffenen Nutzers werden automagisch auf das WWW-Terminal umgelenkt

Sensoren von PRISM

- Die Meldung erfolgt per IDMEF
  (Intrusion Detection Message Exchange Format)
- Mehrere Sensoren sind implementiert:
  - Sophos-Mail-Schnittstelle
  - Intrusion Detection System Snort
  - IDMEF-Aggregator für Snort
  - Manuelle Eingabe über WWW-Schnittstelle
  - DNS (Richtlinienkontrolle)

Mögliche Lösungsdatenbanken

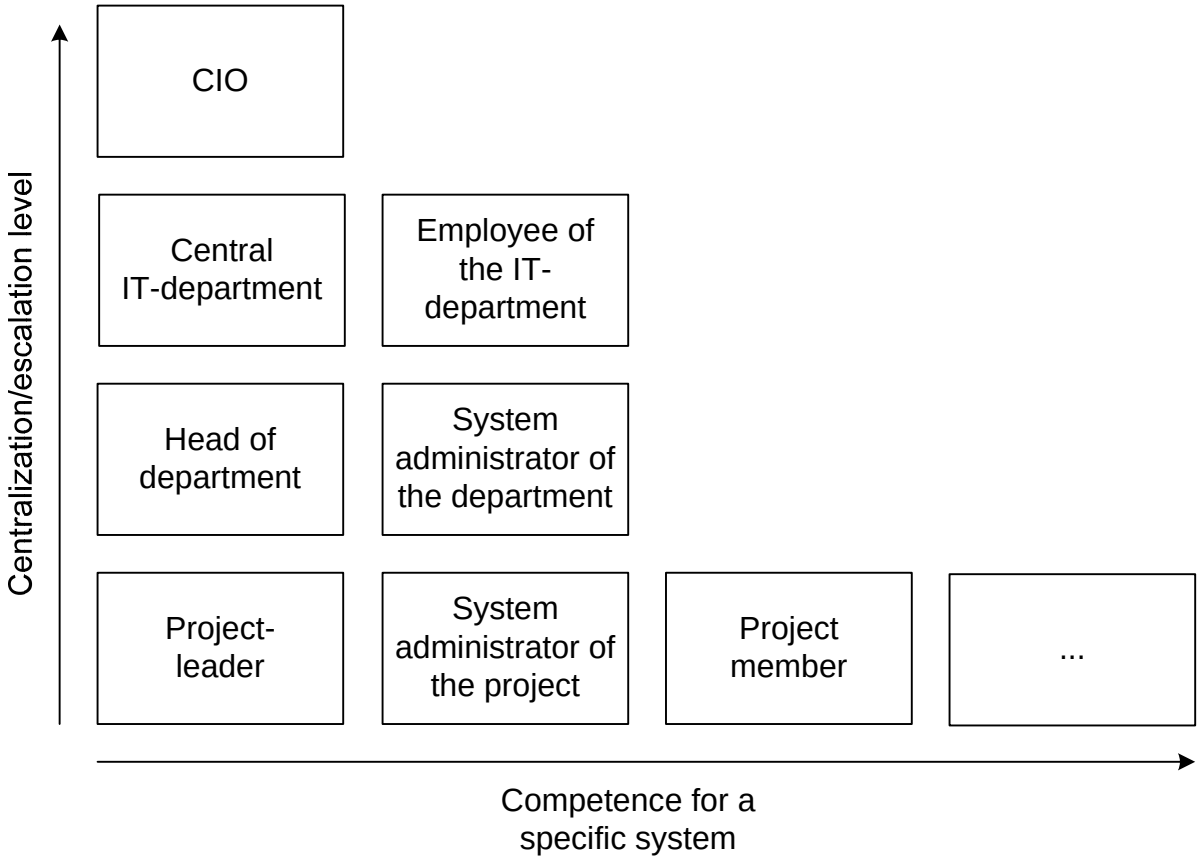
- Eigene Datenbank mit Lösungen (Remedy DB)
- Abfrage von AV-Informationen (Einbettung von Tools)
- API, mehrere Module



Rollen- und Eskalationsmodell

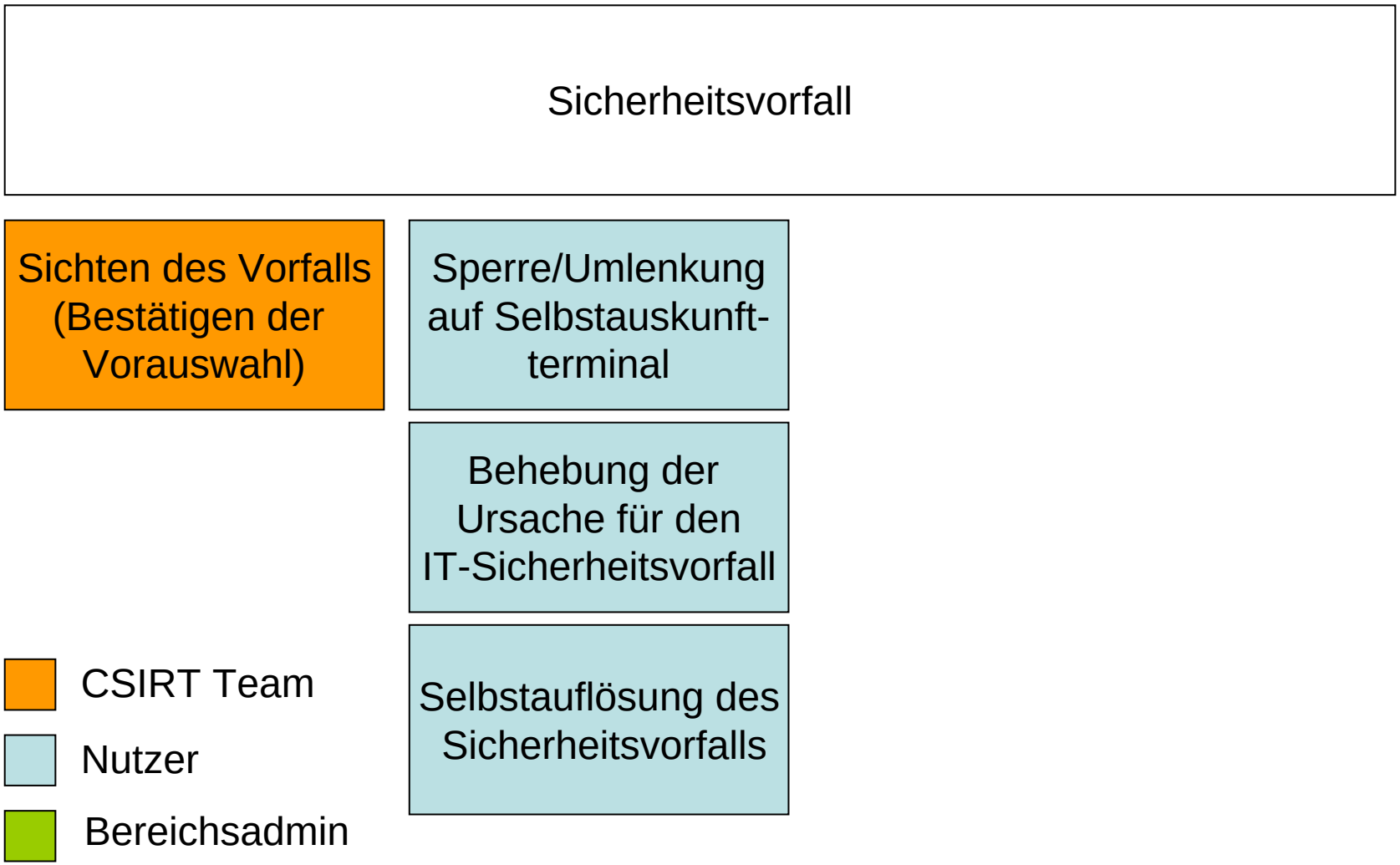
- **Unterschiedliche Rollen:**
  - Endnutzer als Hauptbenutzer des Systems
  - Computer-/Netzwerkadministrator der Einrichtung
  - CSIRT-Administrator
- **Eskalationsmodell**
  - **Class 1 - Level 1** this describes security incidents which have a low risk to the organization.
  - **Class 1 - Level 2** An escalation to level 2 means that the end user was not able to solve the problem himself and that now the computer administrator which is responsible for the organization has to clear the problem.
  - **Class 1 - Level 3** In case the computer administrator cannot fix the problem in level 2, it is possible to increase the level to level 3 and to have a CSIRT administrator supervising the incident.
  - **Class 2 – all Levels** incidents are those which have a significant impact on the organization. These ones should not be solved from users or network administrators but from the CIRT team. A security incident of this class will never be in the scope of an end user.

Beispielhafte hierarchische Verantwortung für IT-Systeme



jochen.kaiser@rrze.uni-erlangen.de

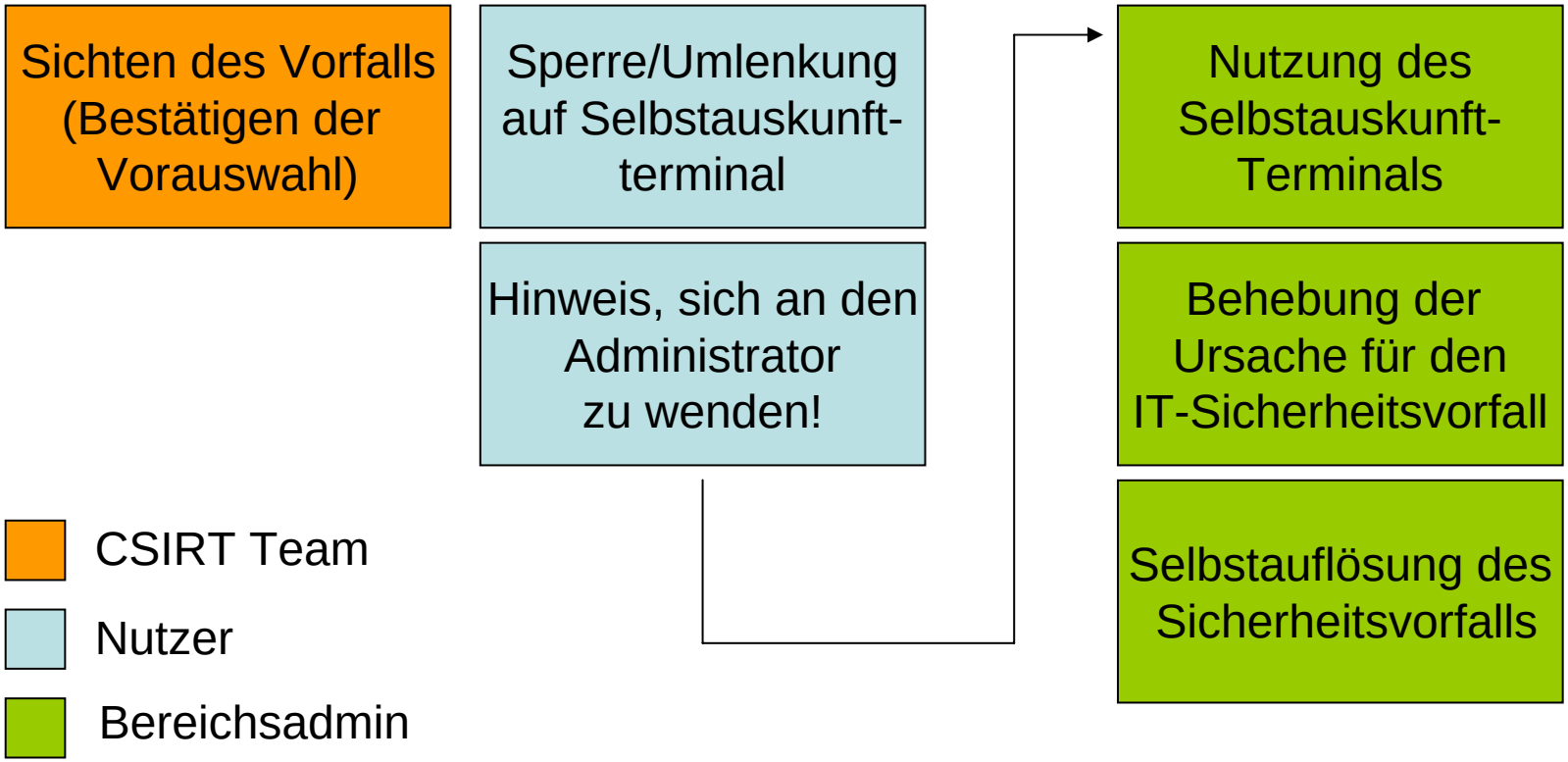
Workflow (keine Eskalation)



jochen.kaiser@rrze.uni-erlangen.de

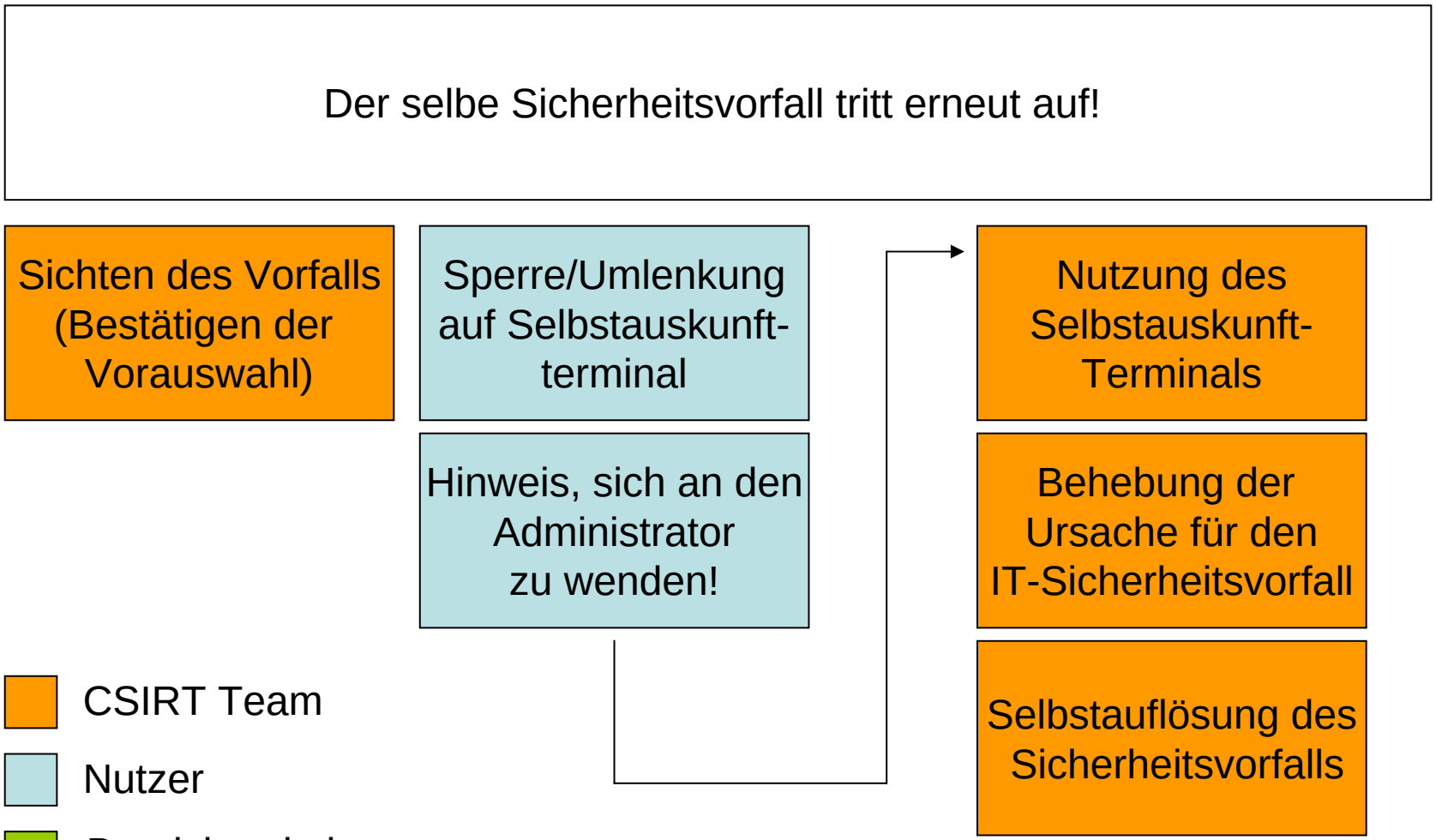
Workflow (Eskalation Stufe 1)

Der selbe Sicherheitsvorfall tritt erneut auf!



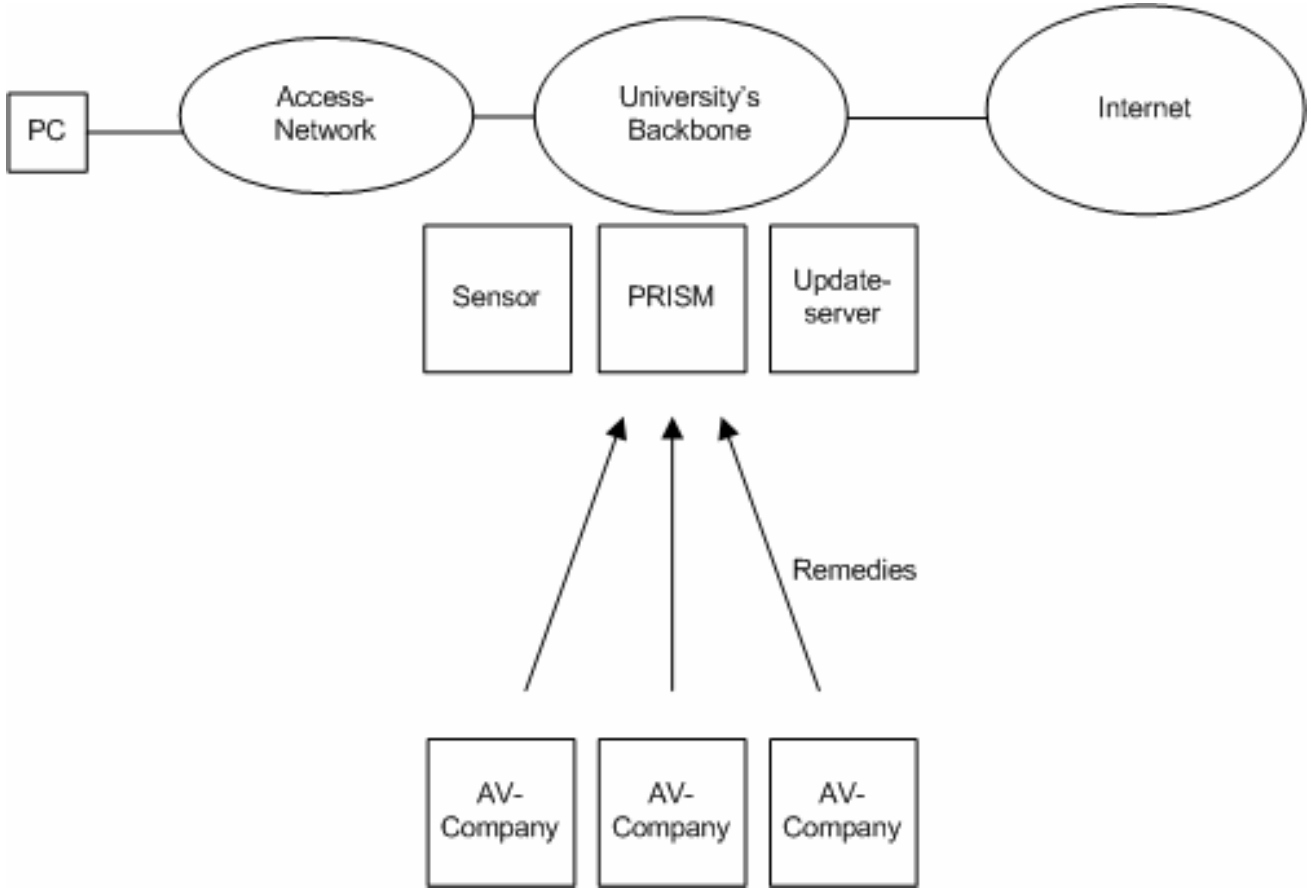
jochen.kaiser@rrze.uni-erlangen.de

Workflow (Eskalation Stufe 2)



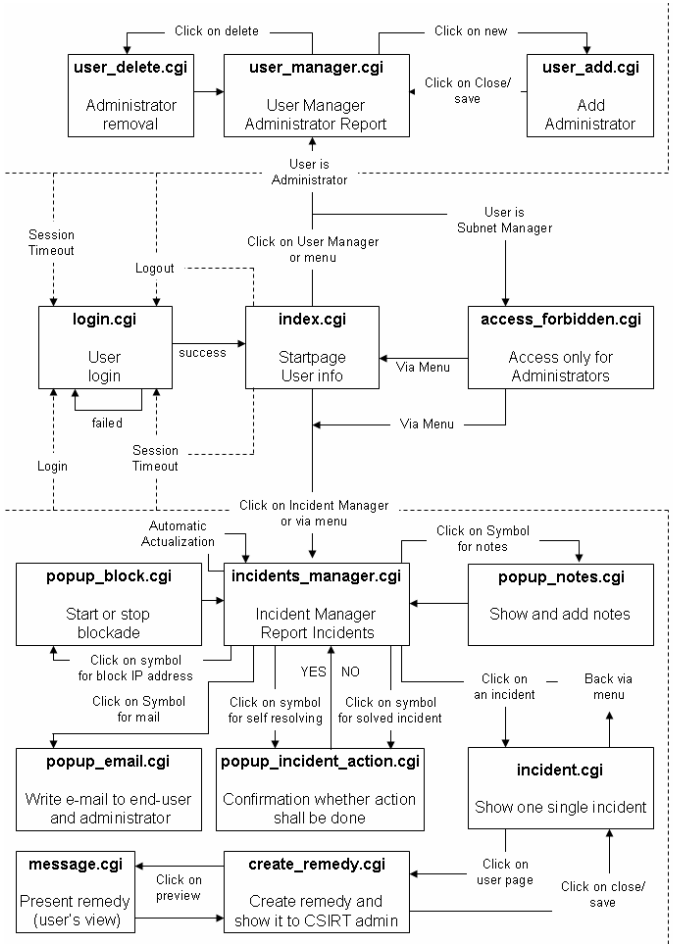
jochen.kaiser@rrze.uni-erlangen.de

Nutzungsszenario: Universität



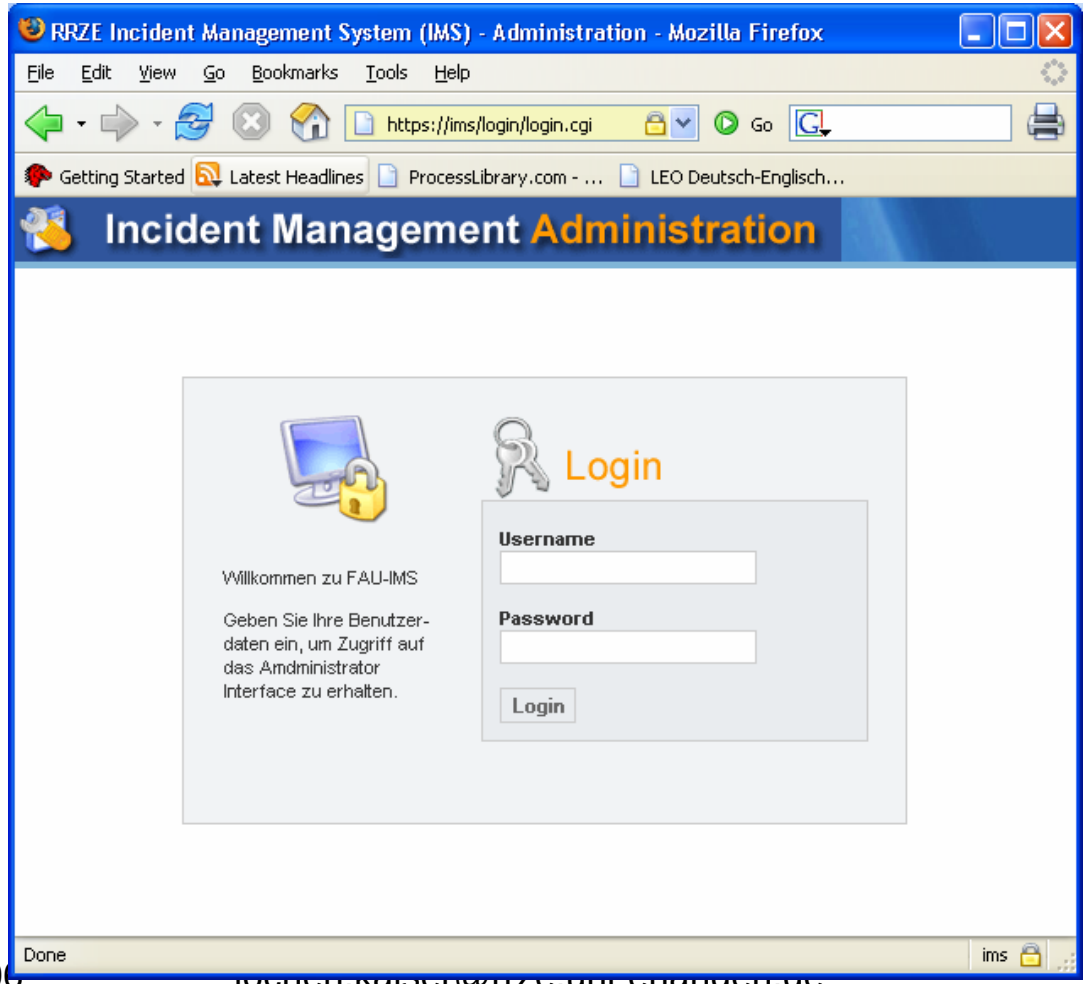
jochen.kaiser@rrze.uni-erlangen.de

Übersicht über die Implementierung

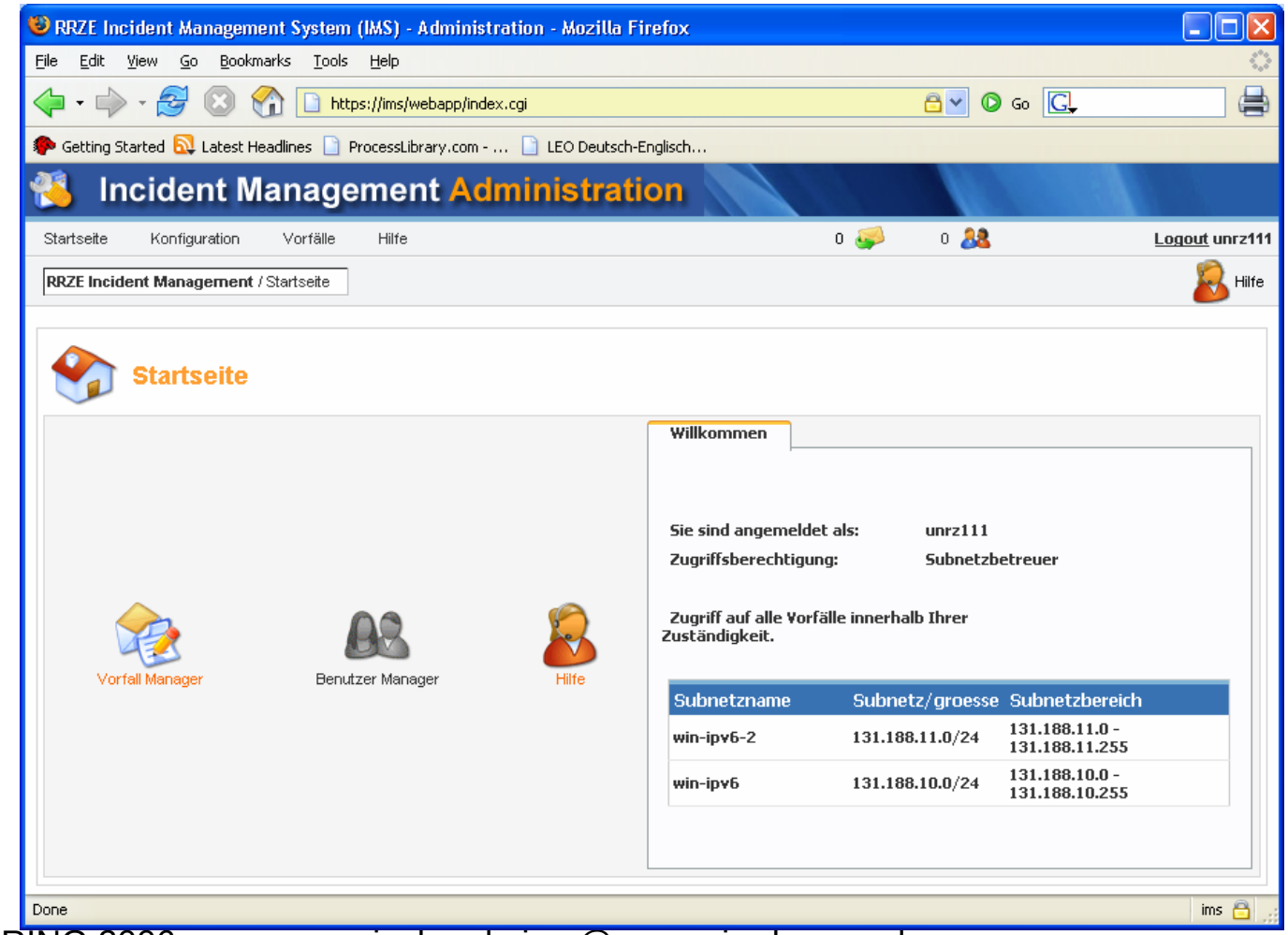


jochen.kaiser@rrze.uni-erlangen.de

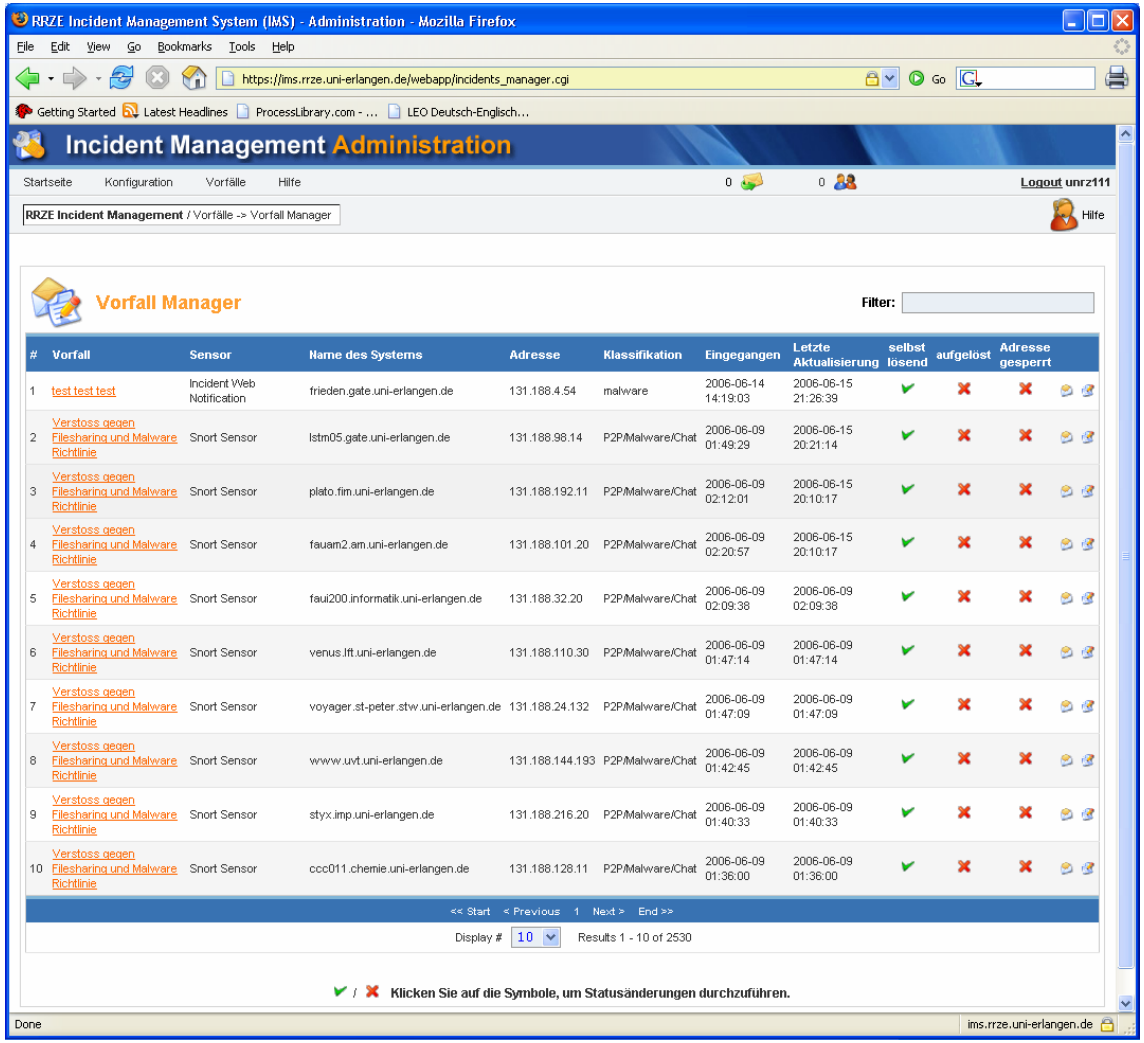
Beispielhafte Sitzung (1) - Login



Beispielhafte Sitzung (2) - Hauptseite

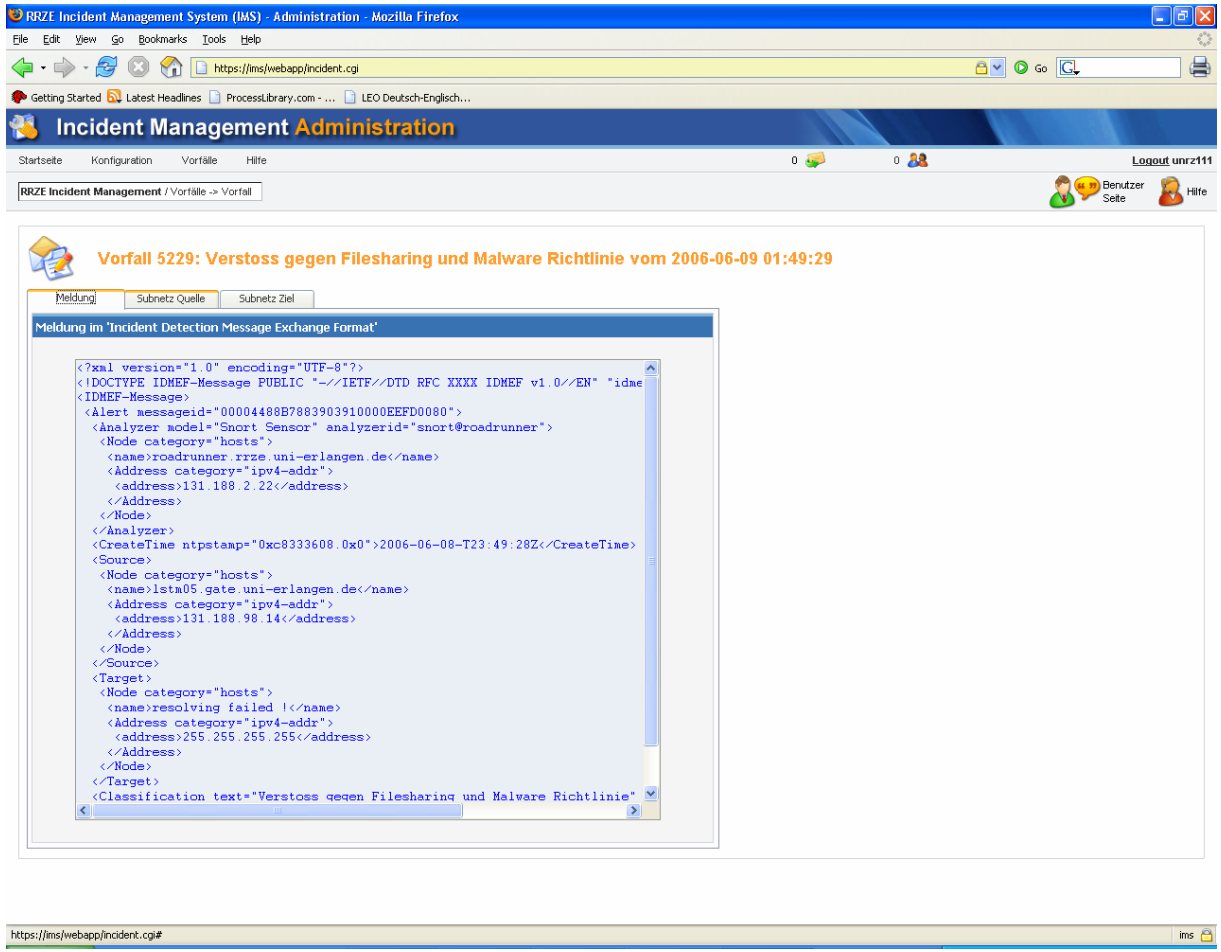


Beispielhafte Sitzung (3) - Vorfallsmanager

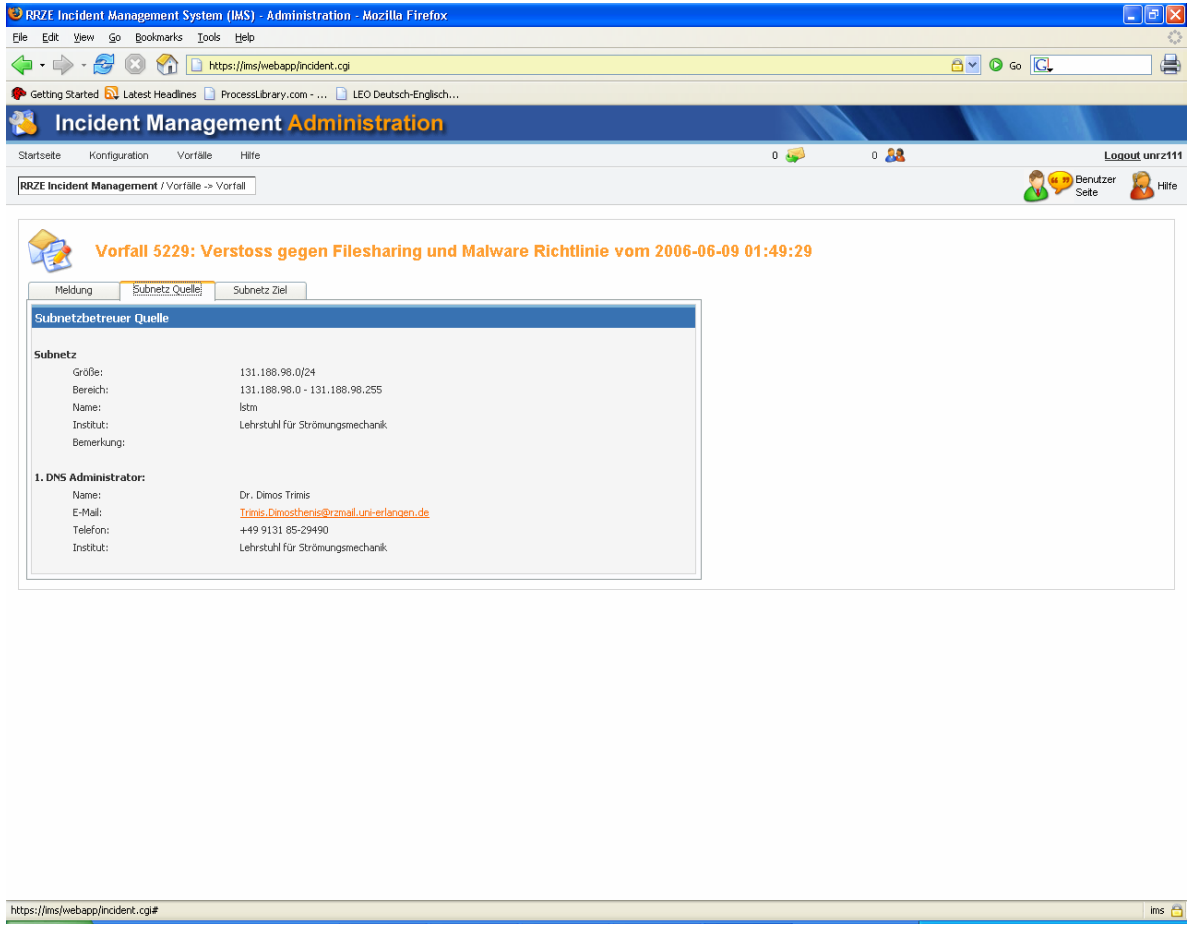


 jochen.kaiser@rrze.uni-erlangen.de

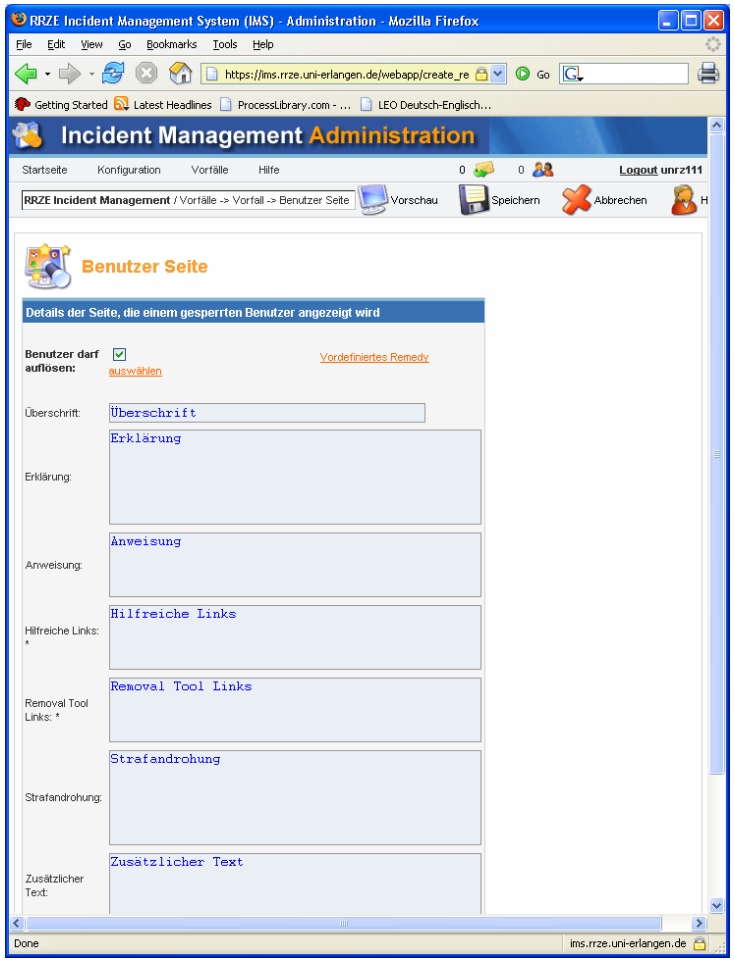
Beispielhafte Sitzung (4) – IDMEF raw



Beispielhafte Sitzung (5) - Ansprechpartner

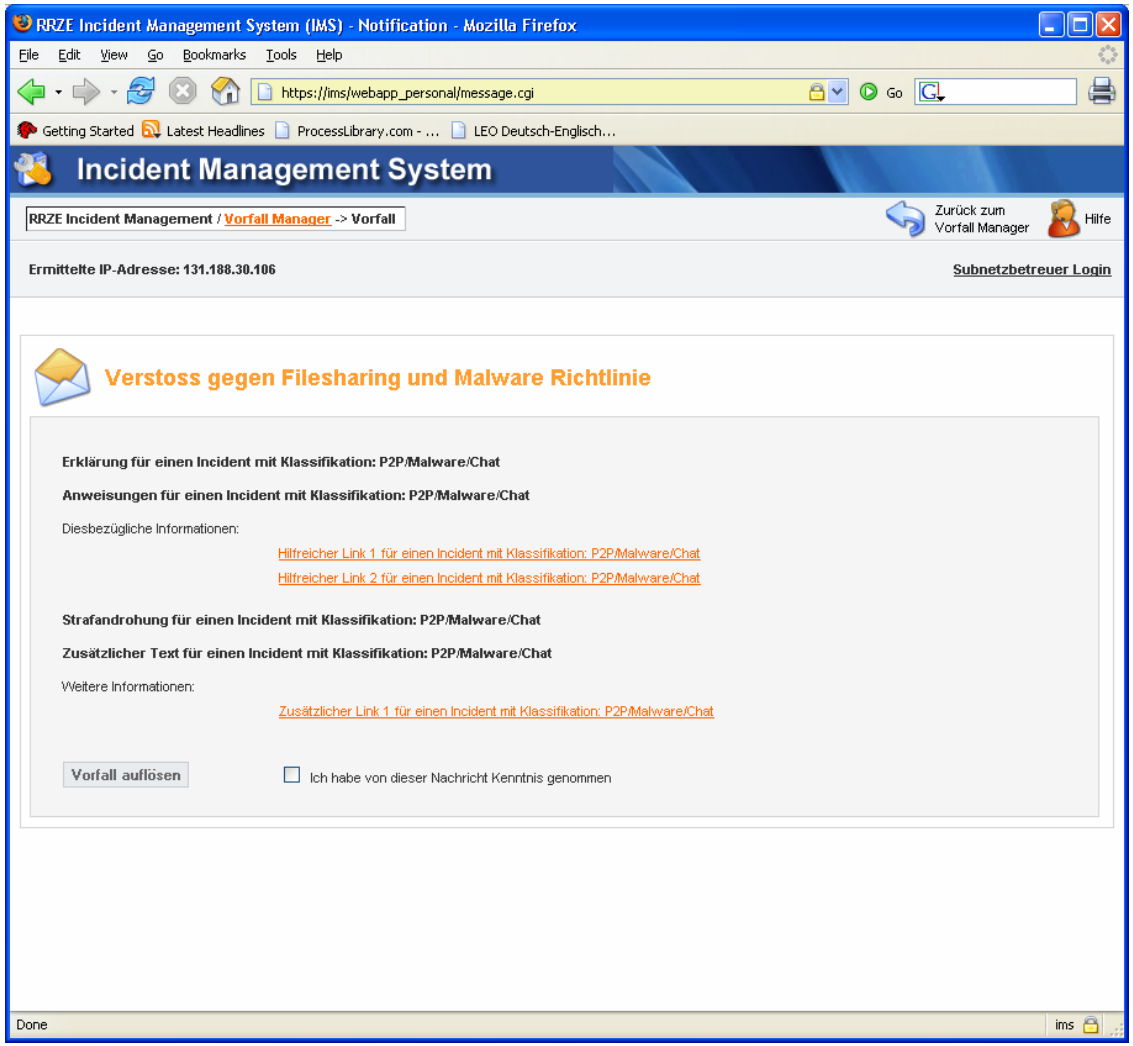


Beispielhafte Sitzung (6) – Erstellen der User-WWW-Seite



Beispielhafte Sitzung (7) Auswahl Lösung

Beispielhafte Sitzung (8) – WWW-Seite



Conclusion und weitere Schritte

- Werkzeug zur Verwaltung von Sicherheitsvorfällen
- Grundsätzliche Funktionsfähigkeit des Systems

Nächste Schritte:

- Implementierung weiterer Bewertungslogiken
- Umrouting der Datenpakete der betroffenen Nutzer im Netzwerk
- Sammeln von Erfahrung im praktischen Einsatz
- Einbettung in größere Untersuchung: „Strategien zur Bewertung von IT-Sicherheitsvorfällen“