

GI SIDAR SPRING 2006

Ein Sicherheitsportal zur Selbstverwaltung und automatischen
Verarbeitung von Sicherheitsvorfällen als Schlüsseltechnologie 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

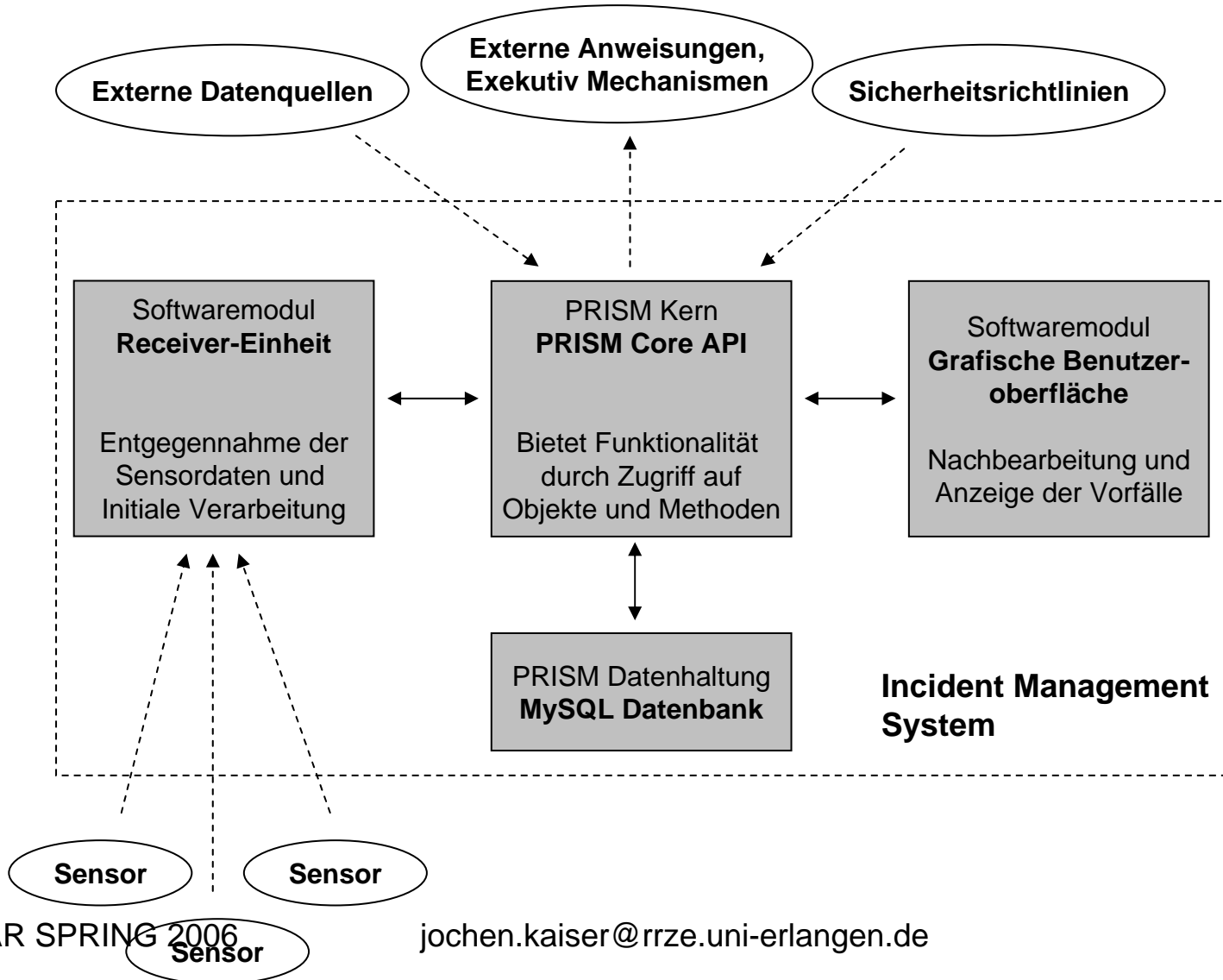
Einsatz von Helpdesksystemen für CSIRT-Aufgaben

- 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

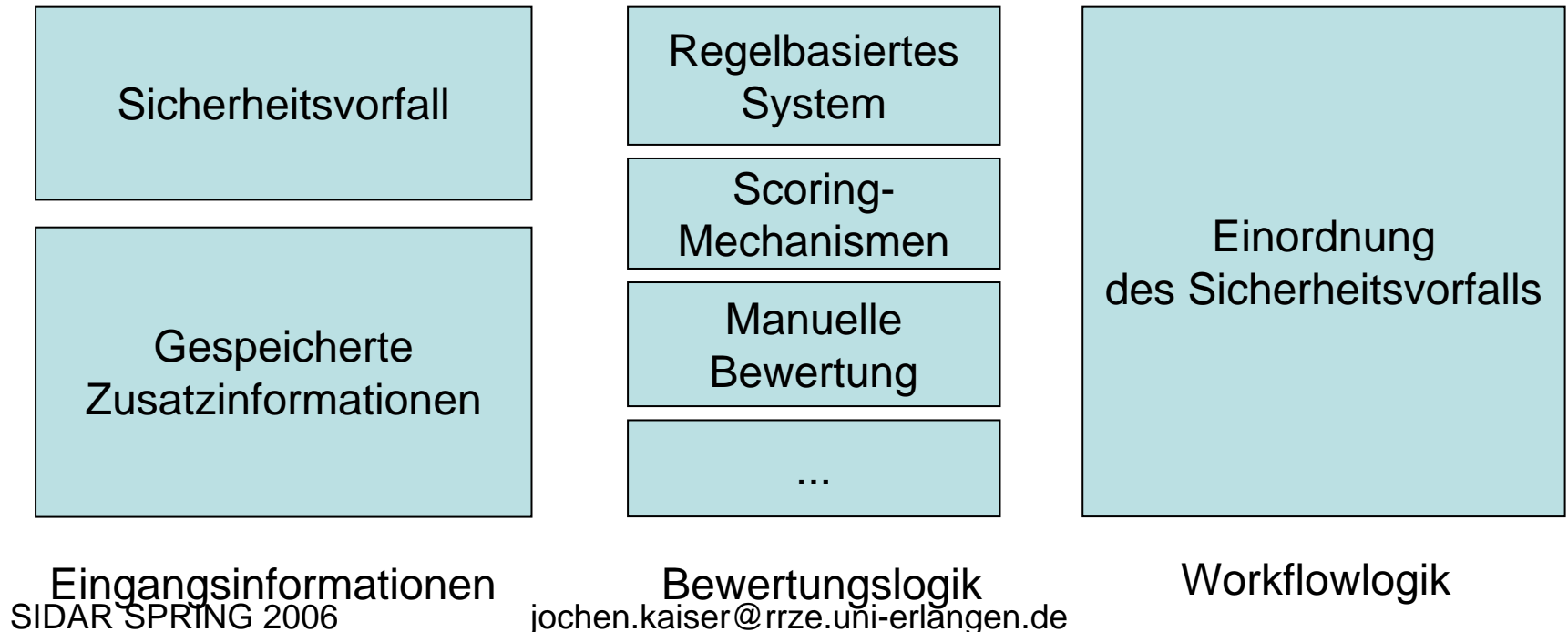
- **Update-Netzwerke**
Eine Menge von Systemen, welche Softwareaktualisierungen für die eingesetzten Netzwerke bereitstellen.
- **Sperrwerkzeug für einzelne Hosts**
Ein Werkzeug muss die folgende Semantik verstehen:
sperre <IP>
entsperre <IP>
Trotz Sperre müssen dennoch die Update-Netzwerke erreichbar 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 automatisch 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

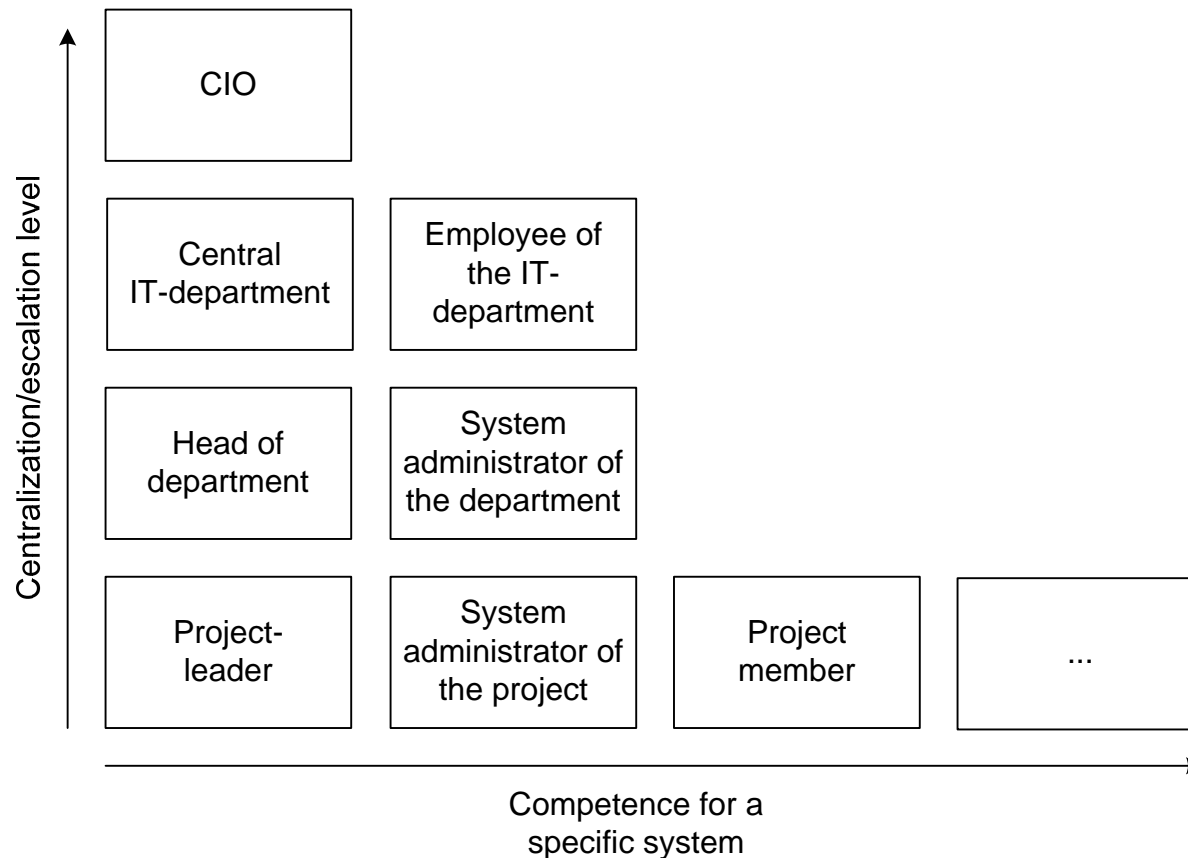
- Eigene Datenbank mit Lösungen (Remedy DB)
- Abfrage von AV-Informationen (Einbettung von Tools)
- API, mehrere Module



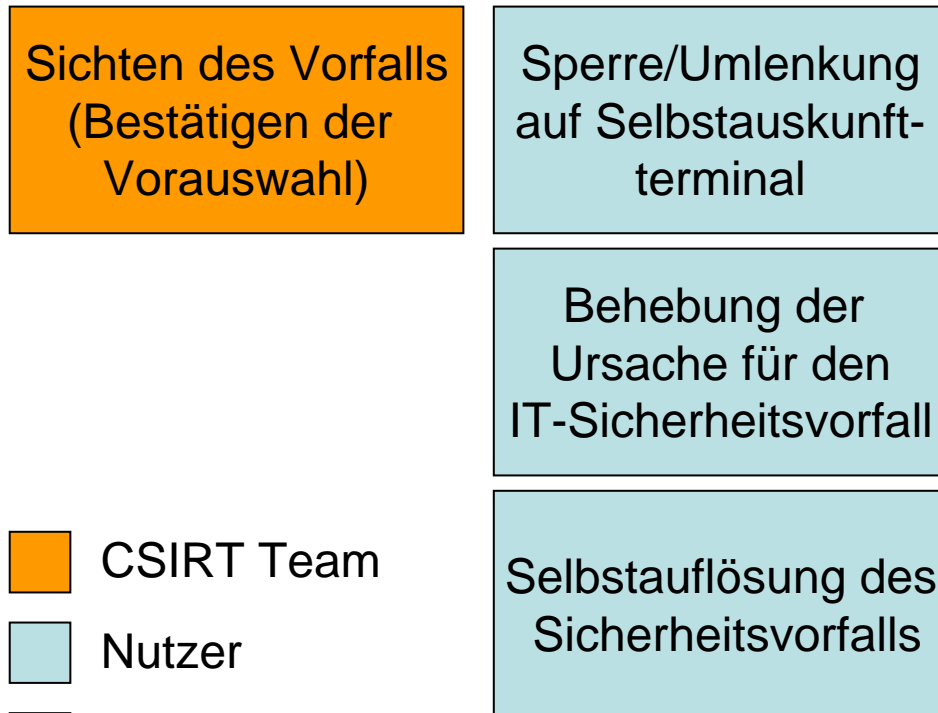
Rollen- und Eskalationsmodell




- **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



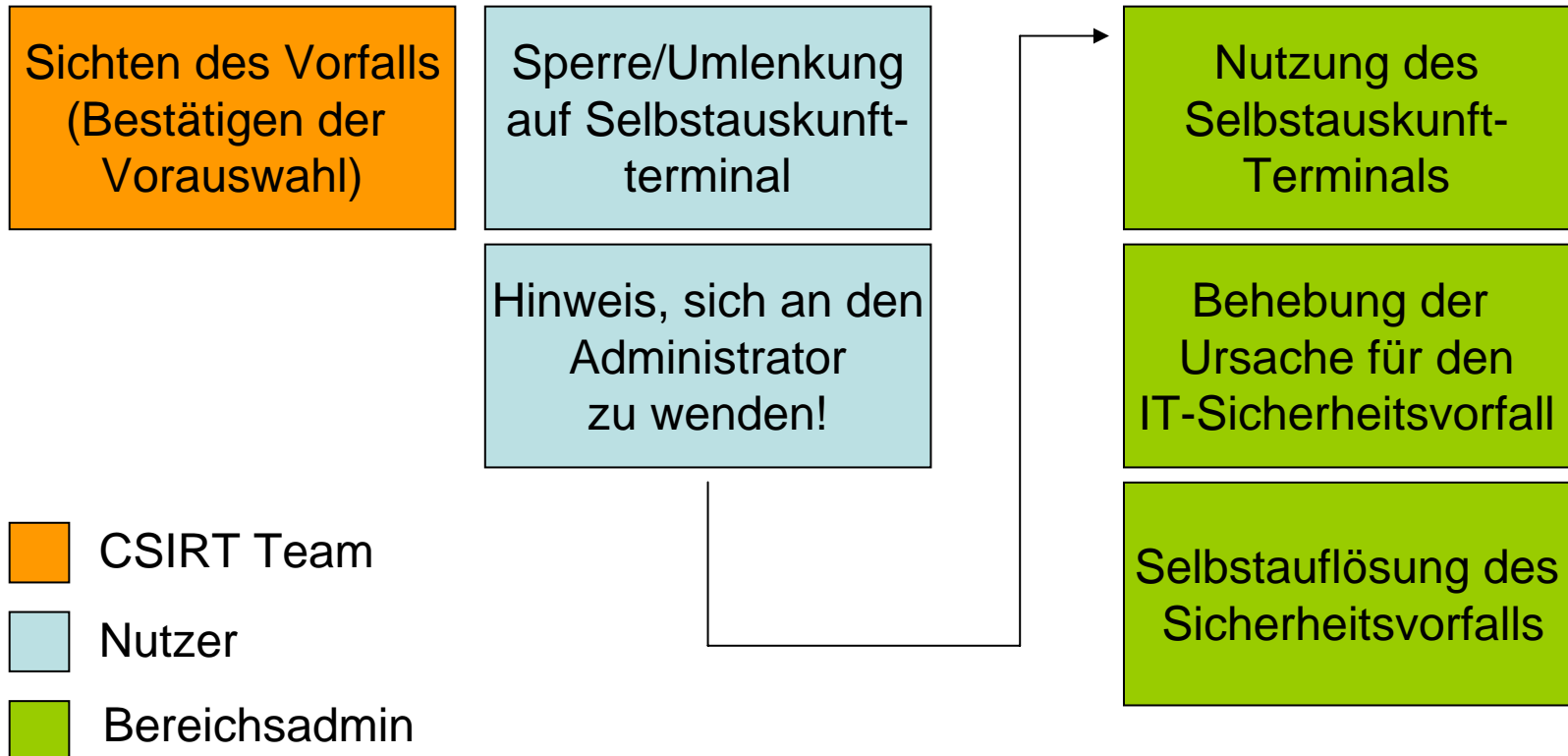
Workflow (keine Eskalation)



-  CSIRT Team
-  Nutzer
-  Bereichsadmin

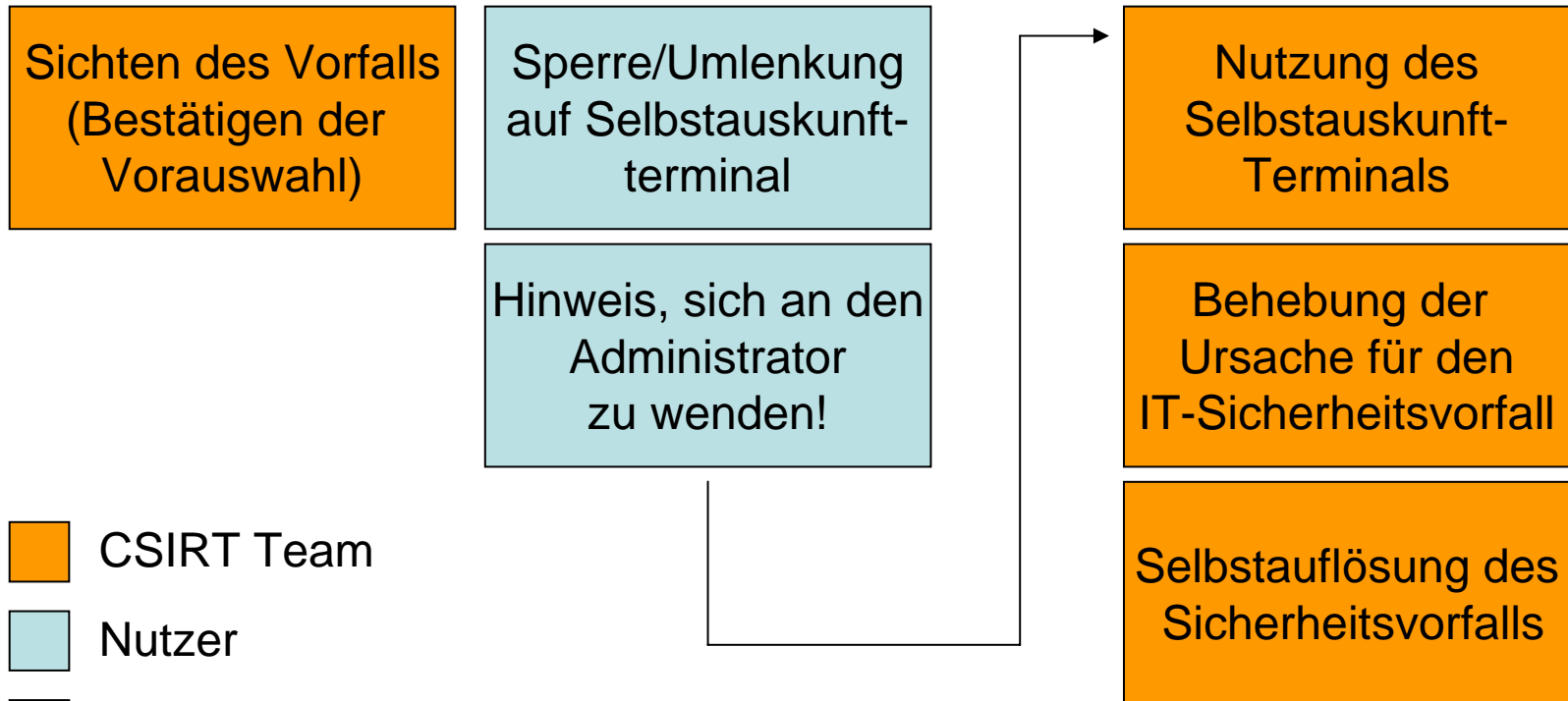
Workflow (Eskalation Stufe 1)

Der selbe Sicherheitsvorfall tritt erneut auf!

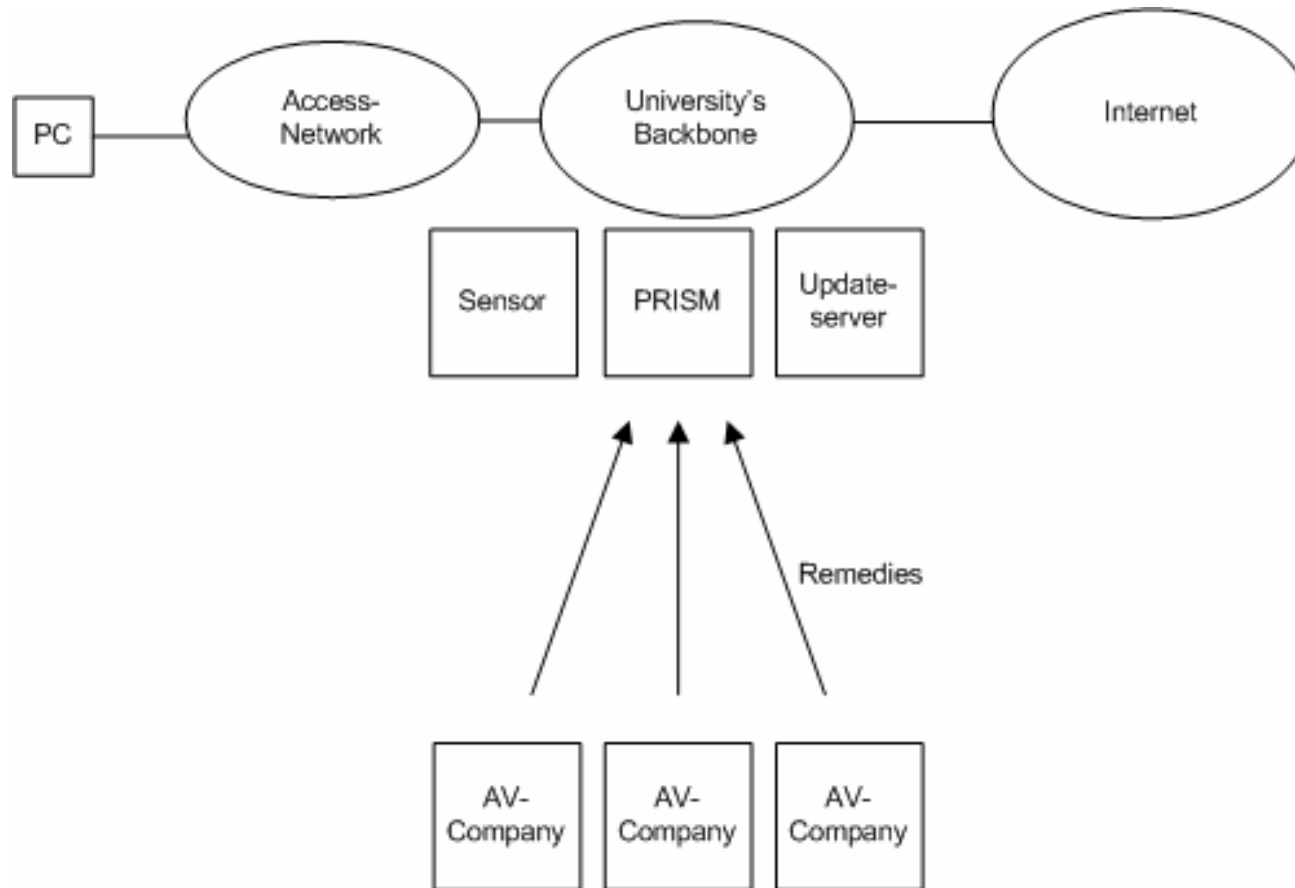


Workflow (Eskalation Stufe 2)

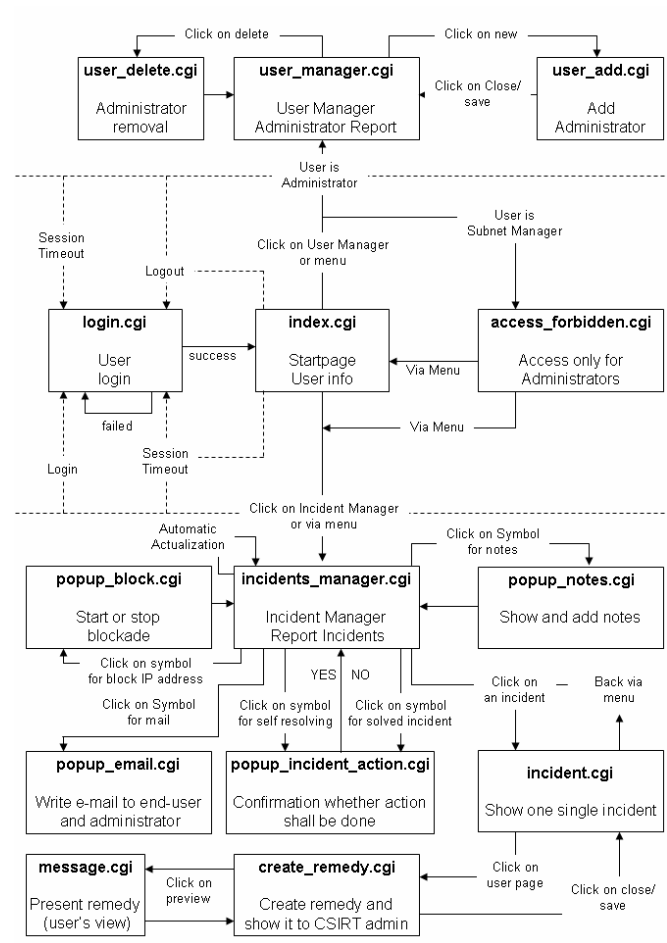
Der selbe Sicherheitsvorfall tritt erneut auf!



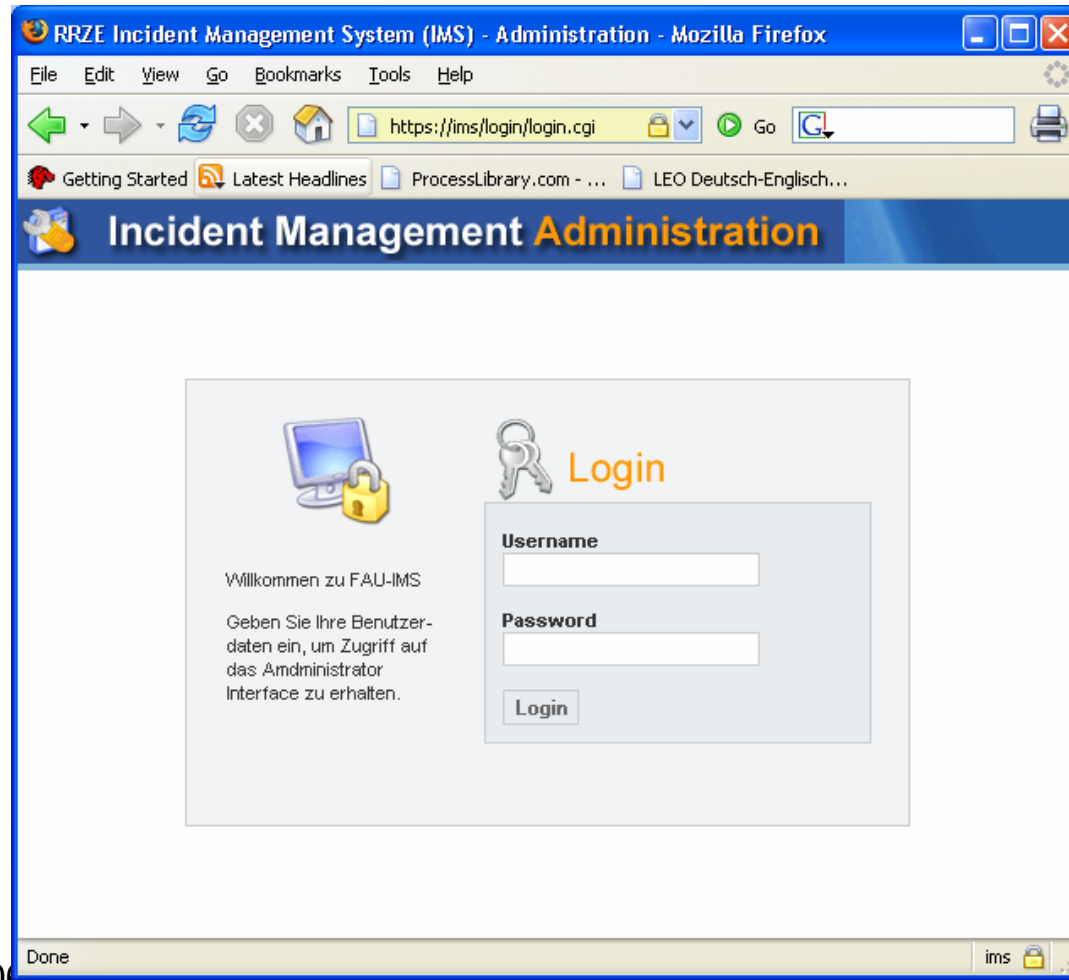
Nutzungsszenario: Universität



Übersicht über die Implementierung



Beispielhafte Sitzung (1) - Login



Beispielhafte Sitzung (2) - Hauptseite

RRZE Incident Management System (IMS) - Administration - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://ims/webapp/index.cgi

Getting Started Latest Headlines ProcessLibrary.com - ... LEO Deutsch-Englisch...

Incident Management Administration

Startseite Konfiguration Vorfälle Hilfe 0 0 Logout unrz111

RRZE Incident Management / Startseite Hilfe

Startseite

Vorfall Manager Benutzer Manager Hilfe

Willkommen

Sie sind angemeldet als: unrz111
Zugriffsberechtigung: Subnetzbetreuer

Zugriff auf alle Vorfälle innerhalb Ihrer Zuständigkeit.

Subnetzname	Subnetz/groesse	Subnetzbereich
win-ipv6-2	131.188.11.0/24	131.188.11.0 - 131.188.11.255
win-ipv6	131.188.10.0/24	131.188.10.0 - 131.188.10.255

Done ims

Beispielhafte Sitzung (3) - Vorfallsmanager

RRZE Incident Management System (IMS) - Administration - Mozilla Firefox

https://ims.rrze.uni-erlangen.de/webapp/incidents_manager.cgi

Incident Management Administration

Startseite Konfiguration Vorfälle Hilfe 0 0 Logout unrz111

RRZE Incident Management / Vorfälle -> Vorfall Manager

Vorfall Manager

Filter:

#	Vorfall	Sensor	Name des Systems	Adresse	Klassifikation	Eingegangen	Letzte Aktualisierung	selbst losend	aufgelöst	Adresse gesperrt	
1	test_test_test	Incident Web Notification	frieden_gate.uni-erlangen.de	131.188.4.54	malware	2006-06-14 14:19:03	2006-06-15 21:26:39	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										
2	test_test_test	Snort Sensor	Istm05_gate.uni-erlangen.de	131.188.98.14	P2P/Malware/Chat	2006-06-09 01:49:29	2006-06-15 20:21:14	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										
3	test_test_test	Snort Sensor	plato_fim.uni-erlangen.de	131.188.192.11	P2P/Malware/Chat	2006-06-09 02:12:01	2006-06-15 20:10:17	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										
4	test_test_test	Snort Sensor	fauam2.am.uni-erlangen.de	131.188.101.20	P2P/Malware/Chat	2006-06-09 02:20:57	2006-06-15 20:10:17	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										
5	test_test_test	Snort Sensor	fau200.informatik.uni-erlangen.de	131.188.32.20	P2P/Malware/Chat	2006-06-09 02:09:38	2006-06-09 02:09:38	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										
6	test_test_test	Snort Sensor	venus.lft.uni-erlangen.de	131.188.110.30	P2P/Malware/Chat	2006-06-09 01:47:14	2006-06-09 01:47:14	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										
7	test_test_test	Snort Sensor	voyager.st-peter.stw.uni-erlangen.de	131.188.24.132	P2P/Malware/Chat	2006-06-09 01:47:09	2006-06-09 01:47:09	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										
8	test_test_test	Snort Sensor	www.uvt.uni-erlangen.de	131.188.144.193	P2P/Malware/Chat	2006-06-09 01:42:45	2006-06-09 01:42:45	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										
9	test_test_test	Snort Sensor	styx.imp.uni-erlangen.de	131.188.216.20	P2P/Malware/Chat	2006-06-09 01:40:33	2006-06-09 01:40:33	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										
10	test_test_test	Snort Sensor	ccc011_chemie.uni-erlangen.de	131.188.128.11	P2P/Malware/Chat	2006-06-09 01:36:00	2006-06-09 01:36:00	✓	✗	✗	
	Verstoss gegen Filesharing und Malware Richtlinie										

<< Start < Previous 1 Next > End >>

Display # Results 1 - 10 of 2530

✓ / ✗ Klicken Sie auf die Symbole, um Statusänderungen durchzuführen.

Done ims.rrze.uni-erlangen.de

Beispielhafte Sitzung (4) – IDMEF raw

Beispielhafte Sitzung (5) - Ansprechpartner

RRZE Incident Management System (IMS) - Administration - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://ims/webapp/incident.cgi

Getting Started Latest Headlines ProcessLibrary.com - ... LEO Deutsch-Englisch...

Incident Management Administration

Startseite Konfiguration Vorfälle Hilfe 0 0 Logout umrz111

RRZE Incident Management / Vorfälle -> Vorfall Benutzer Seite Hilfe

Vorfall 5229: Verstoss gegen Filesharing und Malware Richtlinie vom 2006-06-09 01:49:29

Meldung **Subnetz Quelle** Subnetz Ziel

Subnetzbetreuer Quelle

Subnetz

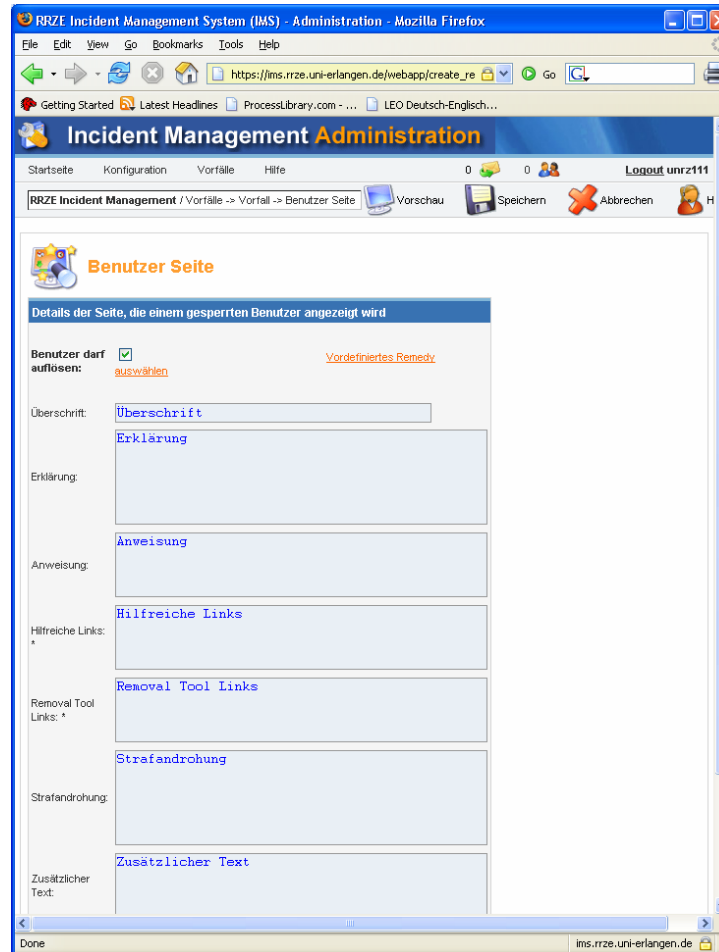
Größe: 131.188.98.0/24
Bereich: 131.188.98.0 - 131.188.98.255
Name: Istm
Institut: Lehrstuhl für Strömungsmechanik
Bemerkung:

1. DNS Administrator:

Name: Dr. Dimos Trimis
E-Mail: Trimis.Dimos@tris@uni-erlangen.de
Telefon: +49 9131 85-29490
Institut: Lehrstuhl für Strömungsmechanik

https://ims/webapp/incident.cgi# ims

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



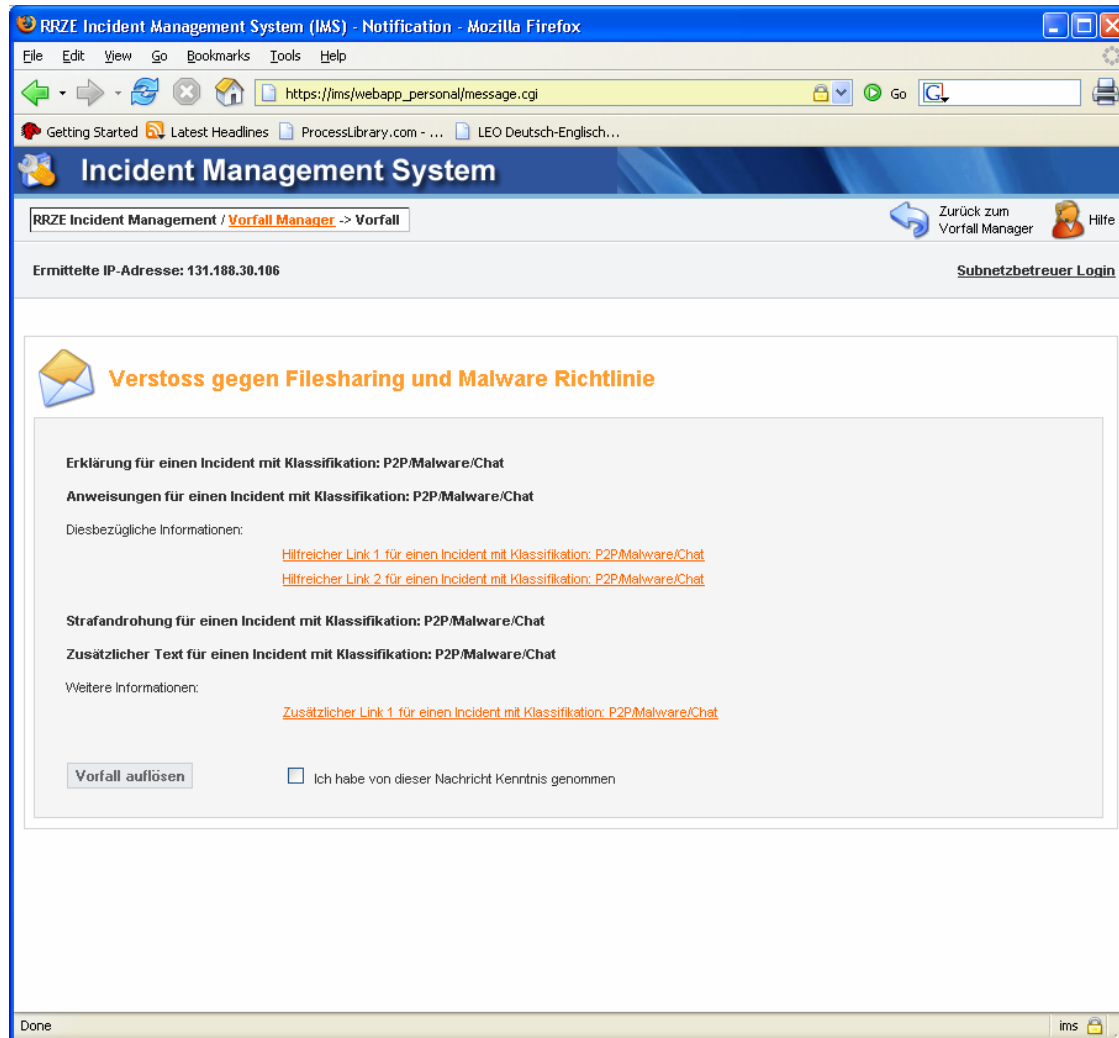
Beispielhafte Sitzung (7) Auswahl Lösung

The screenshot shows a web browser window with the address bar containing `https://ims.rrze.uni-erlangen.de - RRZE Incident Management...`. The main content area is titled "Auswahl eines manuellen Remedies" and contains a form with four radio button options, each with a corresponding dropdown menu:

- Malware
- P2P (dropdown: Überschrift test)
- Portscan (dropdown: 13456xxxxx)
- Kein DNS Eintrag (dropdown: 45454)

At the bottom of the form, there are two buttons: "Speichern Kategorien verwalten" and "Abbrechen Remedies verwalten". The browser's status bar at the bottom shows "Done" on the left and "ims.rrze.uni-erlangen.de" on the right.

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“