Federal Office
for Information Security

BSI

SIRIOS
the Framework for CERTs

Thomas Klingmüller

Federal Office for Information Security (BSI)
Germany

17th FIRST Conference 2005 - Singapore June 26 – July 1, 2005

Abstract

SIRIOS – Framework for CERTs

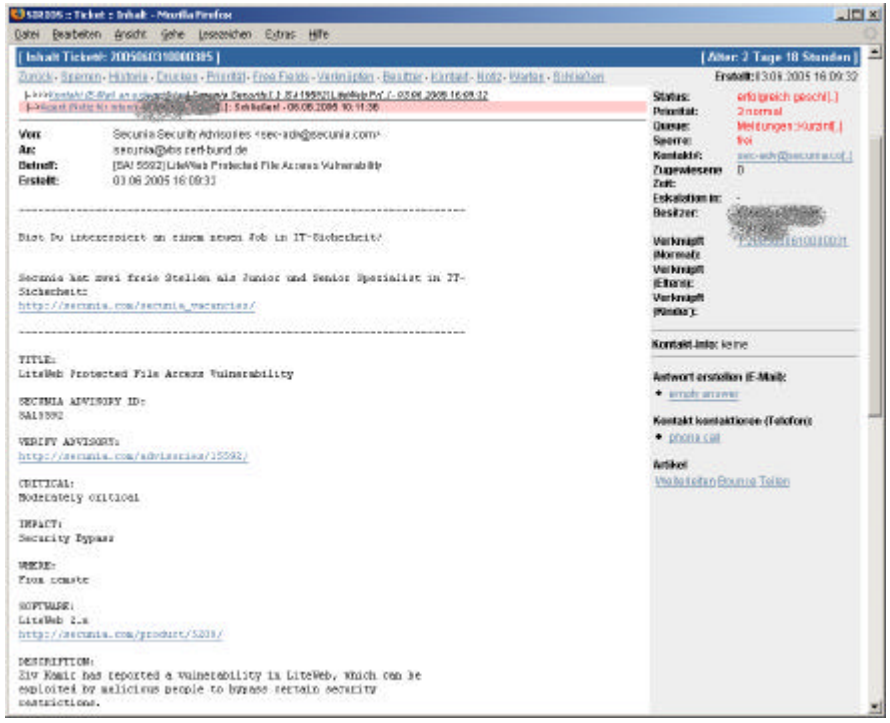
- BSI and CERT-Bund
- SIRIOS – What it is
- SIRIOS – Features
- SIRIOS – Modules
- Incident tracking
- Vulnerabilities
- Further modules
- Download and installation – Where to get it
- SIRIOS at CERT-Bund
- Questions

Framework for CERTs

SIRIOS – **S**ystem for **I**ncident **R**esponse **i**n **O**perational **S**ecurity

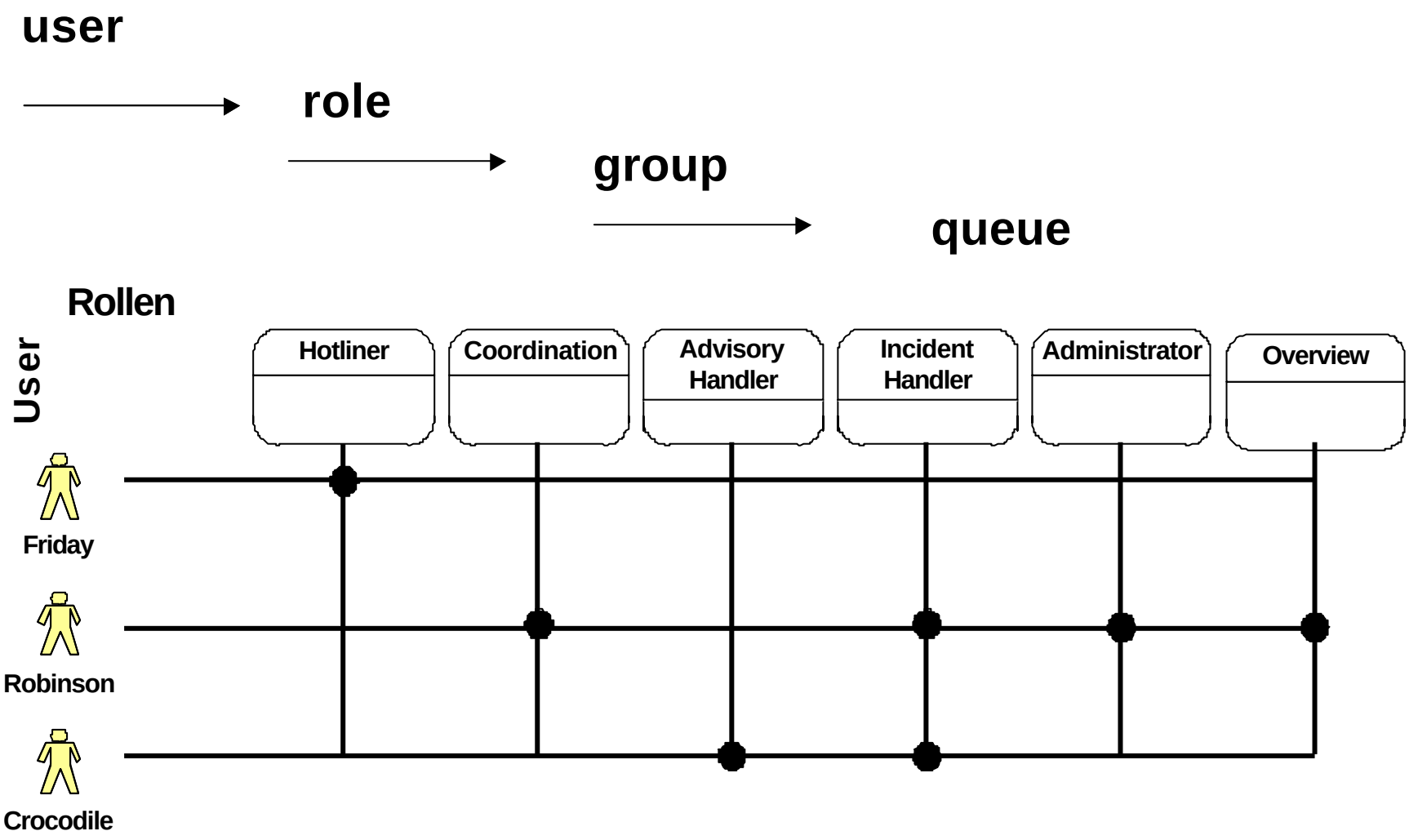
- Internal ticket handling and tracking for CERTs
- Role based workflows for ticket handling
- Processing of vulnerability and incident information
- Incident tracking
- Authoring and publishing system for advisories
- Databases for vulnerability information and artifacts
- Cryptographic support

SIRIOS - Ticket



- Ticket-ID
- From / To
- Subject
- Owner
- History
- Queue
- Krypto-Info
- Age
- Links
- Content
- Escalation status
- (Un-)Lock
- Status
- Contact Information
- Notes
- Print-Preview

Role based workflows



SIRIOS - Features

- Multilanguage support via preconfigured templates
- Platform independent
- Free Open Source Software – GPL*
- Designed with security in mind
- External enhancement: SIRIOS Networks
- Internal enhancement: modular design

*GNU General Public License (**GPL**)

SIRIOS - Modules

- Incident tracking 
- Authoring Advisories 
- Import and export of information using well known standards 
- Checking signatures, encryption, decryption 
- Vulnerability database 
- Artifact database 
- Contact database 
- Monitoring of web sites 
- Administration GUI 
- Multilanguage template based
- Paket manager

Incidents: Incoming

day-to-day CERT Business

- mail handling
- telephone hotline
- Incident reporting
- automated alerts and statistics

SIRIOS - Features

- Filtered inboxes with automated triage
- Telephone to database – with templates
- Role based incident tracking
- IODEF interface
- IDMEF interface

Incidents: processing

day-to-day CERT Business

- Several tools
  - text-editor
  - command line
- Multiple data sources
  - online information
  - databases
  - email
  - paper

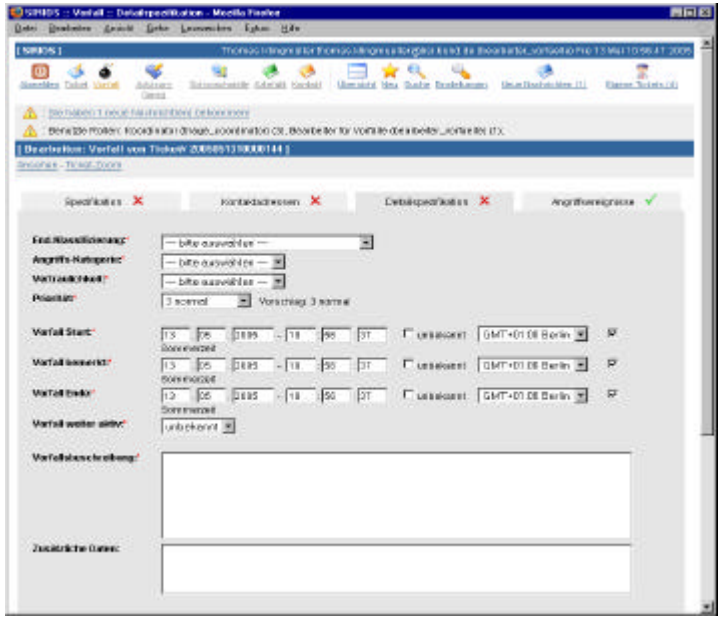
with SIRIOS

- central incident – module
  - Incident tracking
- artifact – database
  - Sourcecode / binaries
  - Logs
  - Any files
- central vulnerability – database
  - Manual input
  - OSVDB objects
  - CVE objects
- contact - database

Incidents: Outgoing

day-to-day CERT Business

- Text-editor
- Mail



with SIRIOS

- Incident – module
  - Anonymising dataobjects
  - Pseudonymising dataobjects
- exchange with IODEF
  - IODEF -> xml-file
  - IDMEF -> xml-file
  - IODEF+IDMEF -> xml-file

Vulnerabilities: Incoming

day-to-day CERT Business

- Maillinglists
- Browser
- Mail
- Telephone

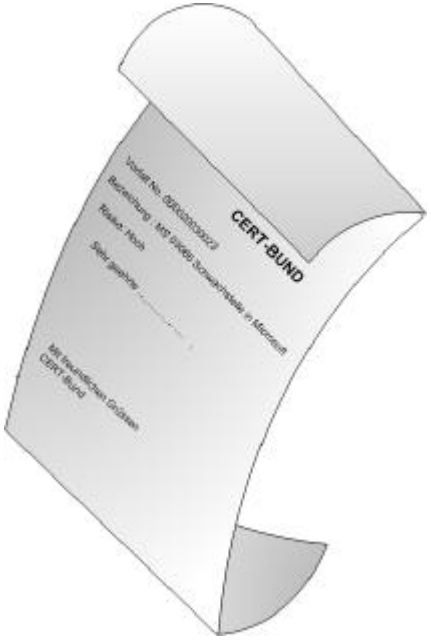
with SIRIOS

- Role based advisory handling
- Workflow-management
- Archivierung aller Maillinglisten
- Multilanguage - templates

Vulnerabilities: Processing

day-to-day CERT Business

- Text – editor
- Self – developed databases
- Internet



with SIRIOS

- Advisory – module
  - Template - GUI for
    - Advisories
    - Virus – alarm/warning
    - Admin – information
  - Quality - check
- Artifact – database
  - Source code
  - files
- Central vulnerability database
  - Vulner. –numbers
  - Risk-level
  - OSVDB / CVE

Vulnerabilities: Outgoing

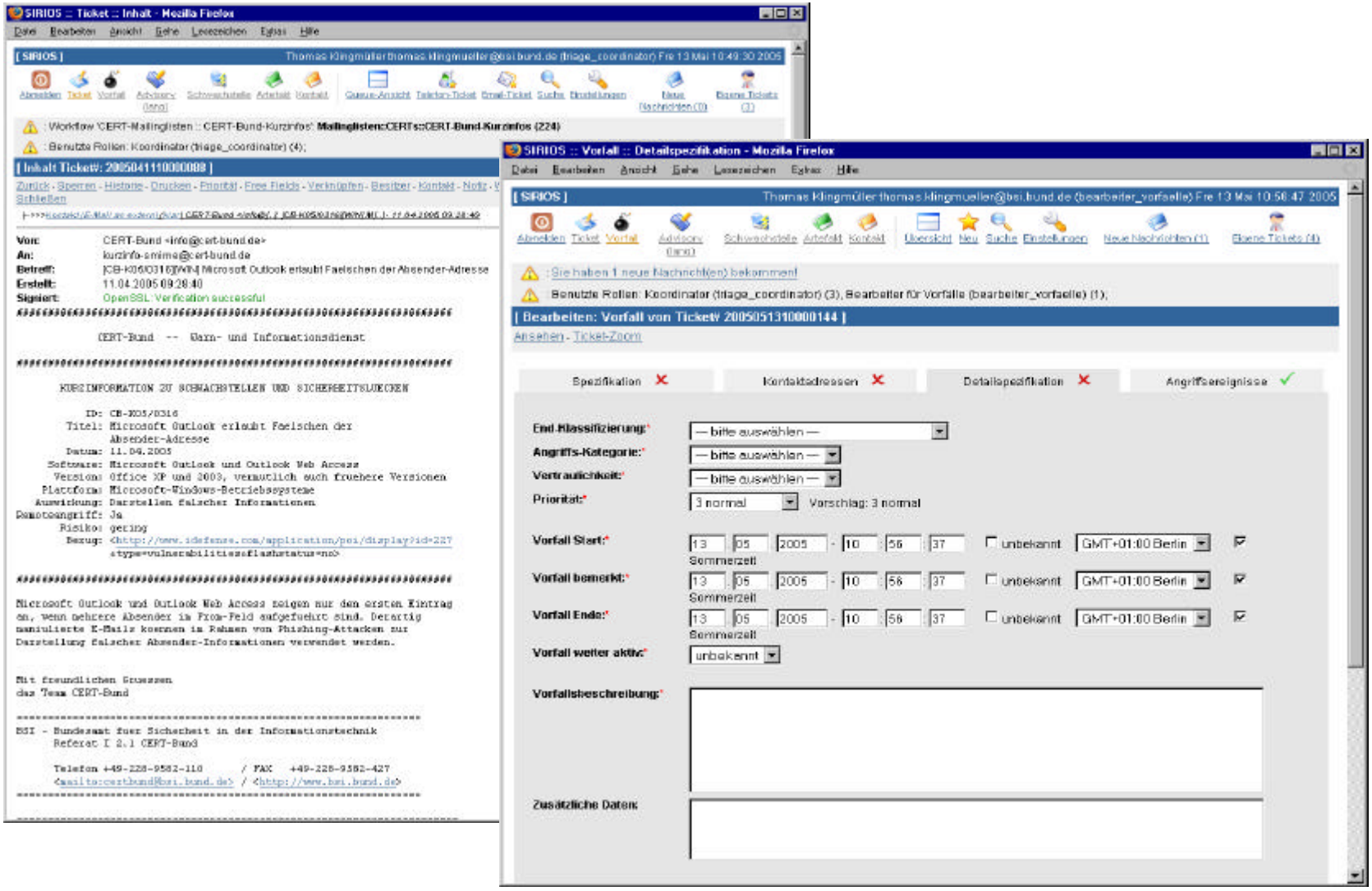
day-to-day CERT Business

- PGP – tools
- S/MIME – tools
- Mail-server

with SIRIOS

- Different advisory formats
  - Long – advisories
  - Short – advisories
  - Virus – alarm/warning
  - Admin – information
- Signing and/or encryption of outgoing information
- Export in EISPP/DAF

in action

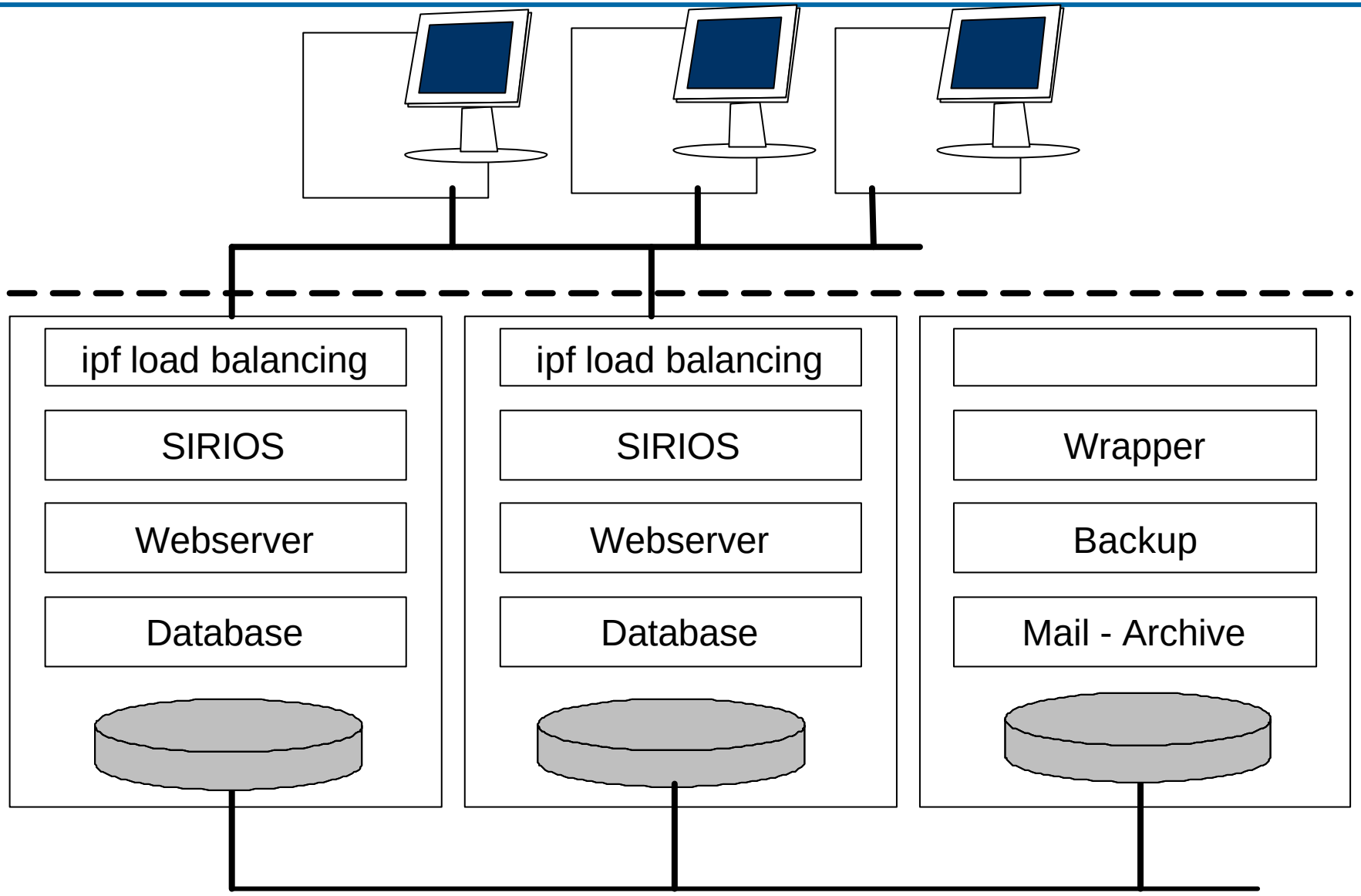

SIRIOS :: Ticket :: Inhalt - Mozilla Firefox
[SIRIOS]
[Inhalt Ticket#: 2005041110000088]
Von: CERT-Bund <info@cert-bund.de>
An: kurzinfo-smime@cert-bund.de
Betreff: [CB-K05/0316][WIN] Microsoft Outlook erlaubt Faelschen der Absender-Adresse
Erstellt: 11.04.2005 09:28:40
Signiert: OpenSSL: Verification successful
CERT-Bund -- Warn- und Informationsdienst
KURZINFORMATION ZU SCHWACHSTELLEN UND SICHERHEITSLUECKEN
ID: CB-K05/0316
Titel: Microsoft Outlook erlaubt Faelschen der Absender-Adresse
Datum: 11.04.2005
Software: Microsoft Outlook und Outlook Web Access
Version: Office XP und 2003, vermutlich auch fruehere Versionen
Plattform: Microsoft-Windows-Betriebssysteme
Auswirkung: Darstellen falscher Informationen
Remotezugriff: Ja
Risiko: gering
Bezug: <http://www.idefense.com/application/poi/display?id=227&type=vulnerabilities&flashstatus=no>
Microsoft Outlook und Outlook Web Access zeigen nur den ersten Eintrag an, wenn mehrere Absender im From-Feld aufgefuehrt sind. Derartig manulierte E-Mails koennen im Rahmen von Phishing-Attacken zur Darstellung falscher Absender-Informationen verwendet werden.
Mit freundlichen Gruessen
das Team CERT-Bund
BSI - Bundesamt fuer Sicherheit in der Informationstechnik
Referat I 2.1 CERT-Bund
Telefon +49-228-9582-110 / FAX +49-228-9582-427
<mailto:certbund@bsi.bund.de> / <http://www.bsi.bund.de>
SIRIOS :: Vorfall :: Detailspezifikation - Mozilla Firefox
[SIRIOS]
Thomas Klingmüller thomas.klingmueller@bsi.bund.de (bearbeiter_vorfaelle) Fre 13 Mai 10:58:47 2005
Sie haben 1 neue Nachricht(en) bekommen!
Benutzte Rollen: Koordinator (triage_coordinator) (3), Bearbeiter für Vorfälle (bearbeiter_vorfaelle) (1),
[Bearbeiten: Vorfall von Ticket# 2005051310000144]
Ansehen - Ticket-Zoom
Spezifikation
Kontaktadressen
Detailspezifikation
Angriffsereignisse
End-Klassifizierung:*
Angriffs-Kategorie:*
Vertraulichkeit:*
Priorität:*
3 normal
Vorschlag: 3 normal
Vorfall Start:*
Vorfall bemerkt:*
Vorfall Ende:*
unbekannt
GMT+01:00 Berlin
Sommerzeit
Vorfall weiter aktiv:*
Vorfallsbeschreibung:*
Zusätzliche Daten:

SIRIOS at CERT-Bund

- Platform – NetBSD 1.6.2
- MySQL
- Apache 2.0
- Perl

- Two Systems in Master-Slave mode
- Load-balancing
- Systemmonitoring with mon
- Full – Backup
- Wrapper – interface for maillinglist-server, webserver (cms)

SIRIOS at CERT-Bund II



Installations – Where to get it

- Source:
  - www.sirios.org (and maillinglists)
  - www.cert-verbund.de/sirios/
- Projectteam
  - CERT-Bund
    - Thomas Klingmüller,
    - Tillmann Werner
  - Helping hand
    - Siemens CERT, Germany
    - DFN-CERT, Germany
    - PRE-CERT, Germany
  - OTRS GMBH, Germany

Federal Office for Information Security

Kontakt

Federal Office for Information Security
(BSI) Germany

Thomas Klingmüller
Section I 2.1 – CERT-Bund
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)1888 9582-561
Fax: +49 (0)1888 9582-90-561

thomas.klingmueller@bsi.bund.de
http://www.bsi.bund.de
http://www.cert-bund.de