Das Datenschutzkonzept des Grid-IDS Projektes und dessen Umsetzung

Dr. Wolfgang Hommel
Dr. Nils gentschen Felde
Felix von Eye
Jan Kohlrausch
Christian Szongott

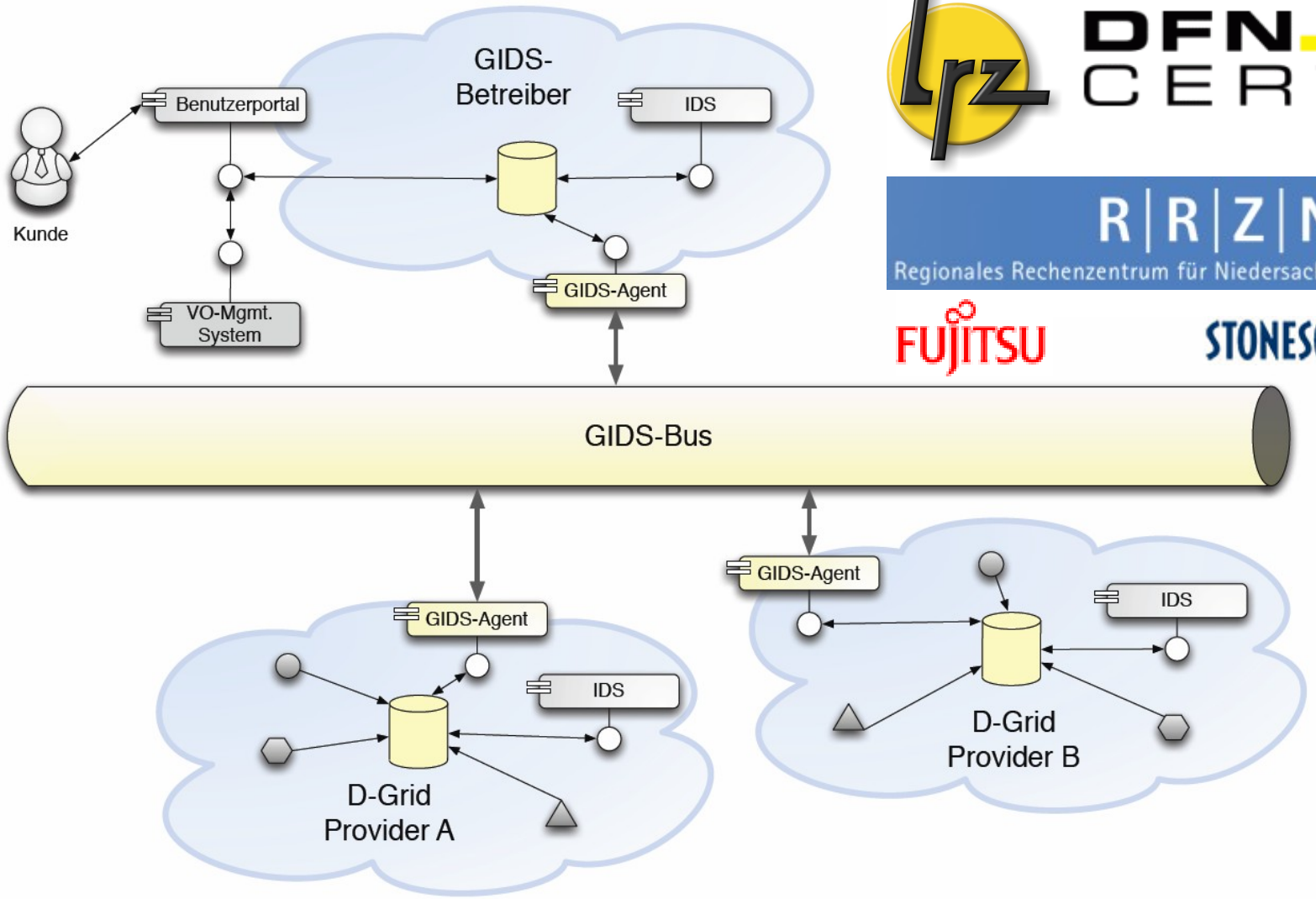
Grid-IDS Projekt

- Ziel: Implementierung und Betrieb eines föderierten IDS für das D-Grid
  - Verbesserte Erkennung von Angriffen durch verteiltes IDS
  - Grid-spezifische Sicht
  - Autonomie der beteiligten Seiten
  - Zentraler Betrieb
- Partner:
  - LRZ-München (Koordination)
  - RRZN Hannover
  - DFN-CERT
  - Stonesoft (assoziiert)
  - Fujitsu (assoziiert)

Aufteilung des GIDS

- Spezifizierung und Implementierung einer föderierten Architektur (GIDS-Bus)
- Anpassung und Einbinden von IDS in die Architektur
- Implementierung von Komponenten für den Betrieb
- Entscheidung für zentrales Datenaustausch-format IDMEF
- Entwurf eines Datenschutzkonzeptes

Übersicht


GIDS-
Betreiber
Benutzerportal
IDS
Kunde
VO-Mgmt.
System
GIDS-Agent
GIDS-Bus
GIDS-Agent
IDS
D-Grid
Provider A
GIDS-Agent
IDS
D-Grid
Provider B

Ziele des Konzeptes

- Schutz sicherheitskritischer Daten
  - Auf der Seite des Betreibers
  - Aus der Sicht der Ressourcenprovider
- Betrieb des GIDS im Einklang mit den rechtlichen Rahmenbedingungen
- Betrifft:
  - Erhebung
  - Verwendung
  - Weitergabe
  - Speicherung der GIDS-Daten
- Zusammenarbeit mit dem DFN-CERT Juristen Dr. Jan Köcher

Grundlagen des Konzeptes

- Sicherheitsanforderungen und Autonomie der am Grid-IDS (GIDS) beteiligten Partner:
  - Welche Informationen gebe ich preis?
  - Wer sieht diese Informationen?

Grundlagen des Konzeptes

- Berücksichtigung der effektiven Erkennung und Korrelation von Angriffen im GIDS

Grundlagen des Konzeptes

- Rechtliche Rahmenbedingungen sind im Bundesdatenschutzgesetz (BDSG) vorgeschrieben.

Rechtliche Grundlagen

- BDSG schränkt Erhebung, Verarbeitung und Weitergabe ***personenbezogener*** Daten ein
- BDSG bietet aber rechtliche Normen:
  - Erhebung und Verarbeitung: Störungsbeseitigung bei Daten-verarbeitenden Systemen
  - Weitergabe: Ermöglichung durch Auftragsdatenverarbeitung
  - Einwilligung der Betroffenen
- Aber: Rechtlicher Graubereich!

Herausforderungen

- Erkennungsleistung des verteilten IDS basiert auf Korrelation der Daten
- Bearbeitung von Vorfällen erfordert Rückverfolgung von Personen
- Rechtliche Anforderungen für Betrieb bindend
- Sicherheitsanforderungen der Ressourcenprovider

Umsetzung

- Anonymisierung oder Pseudonymisierung personenbezogener oder sicherheits-kritischer Daten
- Filterung von IDS-Daten auf der Seite der Ressourcenprovider
- Einschränkungen des Zugriffs beim GIDS-Portal
- Vorgabe einer „sicheren“ Policy
- Schaffung einer rechtlichen Grundlage

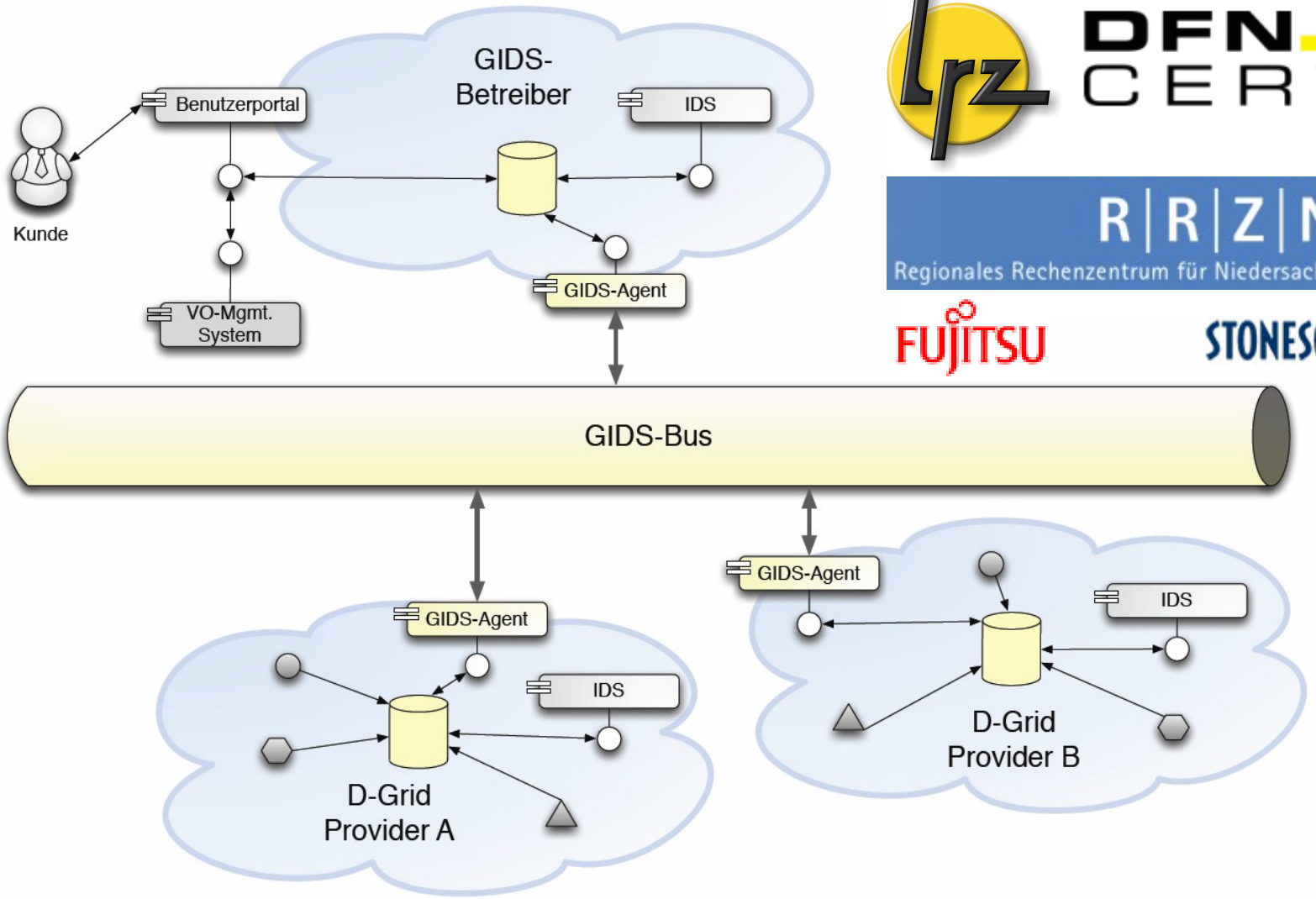
Realisierung: Policy

- Auswertung aller Felder des IDMEF-Datenformates:
  - Potentieller Personenbezug
  - Potentiell sicherheitskritisch für Ressourcenprovider
- Technische Umsetzung durch frei konfigurierbare Policy für IDMEF Export (GIDS-Agent)
- Policy für die Verarbeitung und Speicherfrist der Daten kann vorgegeben werden (*sticky policy*)

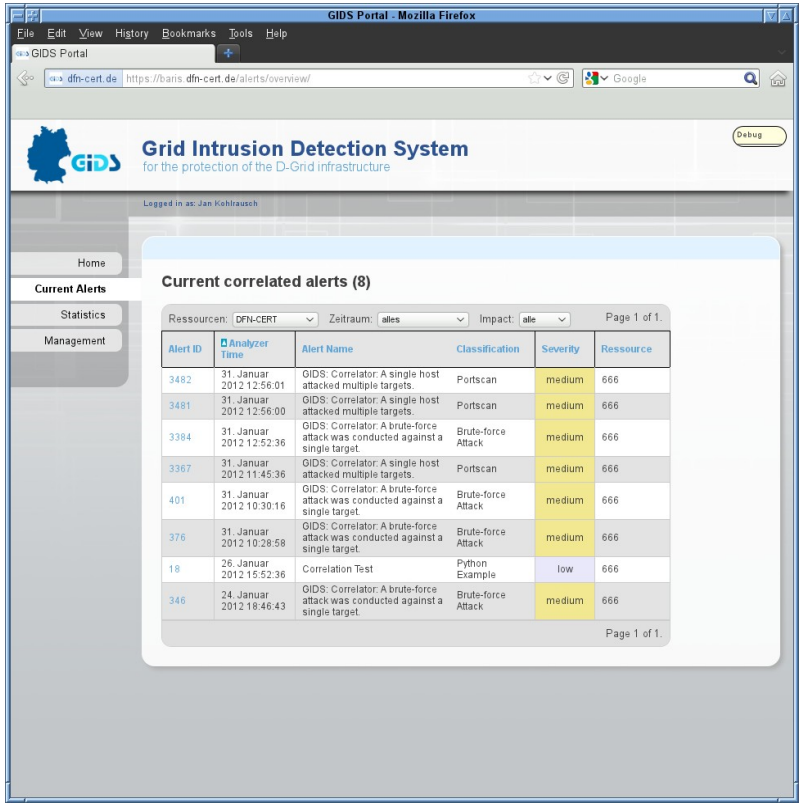
Realisierung: Kooperation

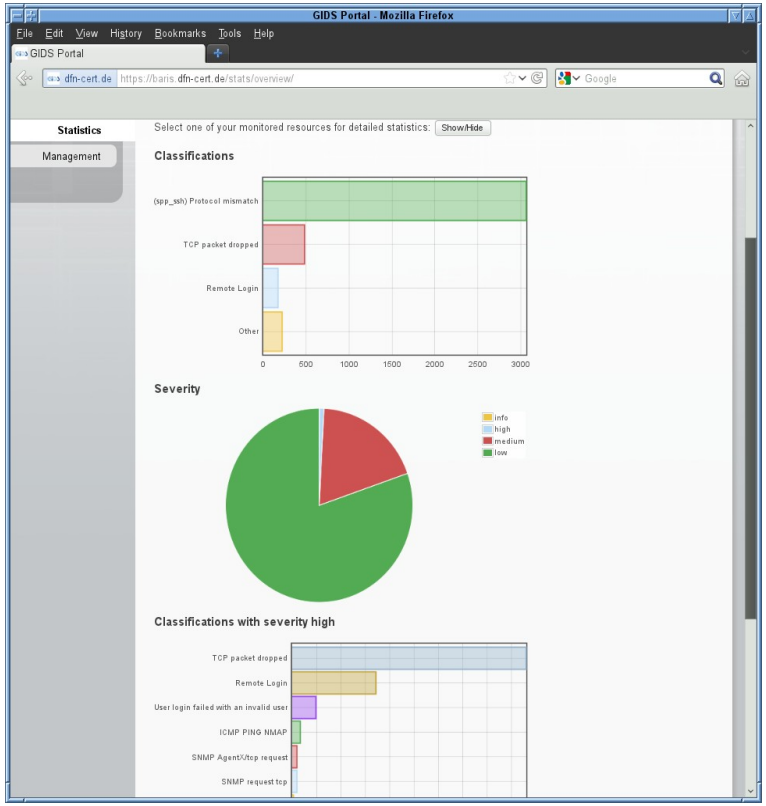
- Mehrfacher, unterschiedlicher Export möglich
- Kooperation mit dem CarmentiS Frühwarnsystem:
  - „Lagebild“ wird zur Verfügung gestellt
  - Kooperationsvereinbarung ist vorhanden

Rückblende


GIDS-
Betreiber
Benutzerportal
IDS
Kunde
VO-Mgmt.
System
GIDS-Agent
GIDS-Bus
GIDS-Agent
IDS
D-Grid
Provider A
GIDS-Agent
IDS
D-Grid
Provider B

Ansichten: GIDS Portal





Zugriff: GIDS Portal

- Authentifizierung über Grid-Zertifikate
- Zugriff nur auf die eigenen Ressourcen
- Ressourcenprovider kann Zugriff für VOs erlauben
- Betreiber hat Zugriff auf alle Daten: *Lagebild*
- Basis: GRRS-Datenbank

Grundlagen: IDMEF

- IDMEF: Intrusion Detection Message Exchange Format
- Struktur durch XML
- Quasi-Standard für viele IDS: Snort, Prelude, OSSEC
- Erzeugung und Bearbeitung durch vorhandene Software, z.B.: Prelude

IDMEF Struktur

- Daten der Sensorik, die den Alarm produziert hat
- Zeitpunkte der Erkennung und Erzeugung des Alarms
- Quelle des Angriffs
  - IP-Adresse
  - Prozess / Service /Benutzer
- Ziel des Angriffs
- Klassifizierung
- Zusätzliche Daten

Beispiel IDMEF

```
<?xml version="1.0" encoding="UTF-8"?>
   <idmef:IDMEF-Message xmlns:idmef="http://iana.org/idmef"
                        version="1.0">
     <idmef:Alert messageid="abc123456789">
       <idmef:Analyzer analyzerid="hq-dmz-analyzer01">
         <idmef:Node category="dns">
           <idmef:name>analyzer01.example.com</idmef:name>
         </idmef:Node>
       </idmef:Analyzer>
       <idmef:CreateTime ntpstamp="0xbc723b45.0xef449129">
         2000-03-09T10:01:25.93464-05:00
       </idmef:CreateTime>
       <idmef:Source ident="a1b2c3d4">
         <idmef:Node ident="a1b2c3d4-001" category="dns">
           <idmef:name>badguy.example.net</idmef:name>
           <idmef:Address ident="a1b2c3d4-002"
                          category="ipv4-net-mask">
             <idmef:address>192.0.2.50</idmef:address>
             <idmef:netmask>255.255.255.255</idmef:netmask>
           </idmef:Address>
         </idmef:Node>
       </idmef:Source>
```

Beispiel: Export-Policy

- [Anonymisieren]
  Address.address = true ; D / LS
  Address.netmask = false ; LS
  Address.vlan-name = false ; LS
  Address.vlan-num = true ; D / LS
  ...
  ...
- [SiteSpezifika]
  gidsRessource = lrz ;
  validUntil = 7 ; # Lebensdauer der Daten

Anonymisierung IDMEF

```
<?xml version="1.0" encoding="UTF-8"?>
   <idmef:IDMEF-Message xmlns:idmef="http://iana.org/idmef"
                        version="1.0">
     <idmef:Alert messageid="abc123456789">
       <idmef:Analyzer analyzerid="hq-dmz-analyzer01">
         <idmef:Node category="dns">
           <idmef:name>analyzer01.example.com</idmef:name>
         </idmef:Node>
       </idmef:Analyzer>
       <idmef:CreateTime ntpstamp="0xbc723b45.0xef449129">
         2000-03-09T10:01:25.93464-05:00
       </idmef:CreateTime>
       <idmef:Source ident="a1b2c3d4">
         <idmef:Node ident="a1b2c3d4-001" category="dns">
           <idmef:name>badguy.example.net</idmef:name>
           <idmef:Address ident="a1b2c3d4-002"
                          category="ipv4-net-mask">
             [illegible]
             <idmef:netmask>255.255.255.255</idmef:netmask>
           </idmef:Address>
         </idmef:Node>
       </idmef:Source>
```

Pseudonymisierung IDMEF

```
<?xml version="1.0" encoding="UTF-8"?>
   <idmef:IDMEF-Message xmlns:idmef="http://iana.org/idmef"
                        version="1.0">
     <idmef:Alert messageid="abc123456789">
       <idmef:Analyzer analyzerid="hq-dmz-analyzer01">
         <idmef:Node category="dns">
           <idmef:name>analyzer01.example.com</idmef:name>
         </idmef:Node>
       </idmef:Analyzer>
       <idmef:CreateTime ntpstamp="0xbc723b45.0xef449129">
         2000-03-09T10:01:25.93464-05:00
       </idmef:CreateTime>
       <idmef:Source ident="a1b2c3d4">
         <idmef:Node ident="a1b2c3d4-001" category="dns">
           <idmef:name>badguy.example.net</idmef:name>
           <idmef:Address ident="a1b2c3d4-002"
                          category="ipv4-net-mask">
             <idmef:address>10.2.2.50</idmef:address>
             <idmef:netmask>255.255.255.255</idmef:netmask>
           </idmef:Address>
         </idmef:Node>
       </idmef:Source>
```

Fragen?

Projektdetails:

www.grid-ids.de

Kontakt:

GIDS-Team
<gids@d-grid.de>