TKÜV mit SPONTS

Kurt Huwig
Vorstand iKu Systemhaus AG
Leiter Entwicklungsabteilung
http://www.iku-ag.de/

iKu Systemhaus AG

- gegründet 1997
- seit 2002 Aktiengesellschaft
- 10 Mitarbeiter
- Geschäftsfelder
  - Linux
  - Java
  - Schulung
  - Beratung/Support

iKu Systemhaus AG

Linux

- Villeroy & Boch - E-Mail-Cluster
- SIKB – Firewall

iKu Systemhaus AG

Java

- Ericsson
- Saar-Energie, Dillinger Hüttenwerke
- Karlsberg

iKu Systemhaus AG

Schulung

- SUSE zertifizierte Linux Trainer
- LPI zertifizierte Techniker
- eigene Schulungsunterlagen
- Schulungen seit 1998

iKu Systemhaus AG

Beratung/Support

- Cluster
- HA-Systeme
- Firewall
- VPN/Kryptografie

iKu Systemhaus AG

SPONTS

- SMTP-Proxy
- Entwicklung seit Anfang 2003
- vorgestellt auf CeBIT 2004
- eigenes Modul „TKÜV“
  - keine Entwicklung ausschließlich für TKÜV
  - zukunftssicher

Modulares Konzept

- MTA-Funktionalität
  - SSL, TLS und SMTP AUTH
  - Virenschutz

Modulares Konzept

- erweitert durch Module
  - UCE
  - UMS
  - Replay
  - Journal
  - TKÜV
- Freischaltung über Lizenzschlüssel
  - Teststellung möglich

iKu Systemhaus AG

Datenhaltung in SQL

- hohe Performance
- leichte Wartung, Backup
- leichte Erweiterbarkeit
- leichte Anbindung an bestehende Systeme
- ANSI92 SQL über JDBC
- Beispiel
  - Benutzer-/Domain-spezifische Virenscanner

Konfiguration über Web-GUI

- 3 Adminstrationsstufen
  - Admin
  - Domain-Admin
  - Benutzer
- für Benutzer keine Datenbank notwendig

iKu Systemhaus AG

Java

- keine Buffer Overflows möglich
- mehr als ausreichende Performance
  - > 800.000 Mails/Tag auf 533MHz
- Plattform unabhängig
- getestet auf
  - FreeBSD
  - HP-UX
  - Linux
  - Windows

iKu Appliance

- optional, aber empfohlen
- komplett passive Hardware
- passiv gekühlte CPU (533 Mhz)
- Flash-Chip statt Festplatte (256 MB)
- hohe Ausfallsicherheit

iKu Systemhaus AG

iKu Appliance

- gehärtetes Linux
- 8 MB Größe
- Zugriff/Updates per SSH und SCP
- einsatzbereit vorinstalliert
- Mini-ITX: 570€
- 19“ 1 HE rack-mount: 820€

iKu Systemhaus AG

Leistung

- Standard
  - 800.000 SMTP-Verbindungen pro Tag (38kB)
  - 1.700.000 POP3-Verbindungen pro Tag (38kB)
- 200MB Speicherkapazität
- Erweiterung
  - IDE-Festplatte
  - RAID-System
  - schnellere Prozessoren

UCE – Spam Abwehr

- Spamassassin
- Realtime blacklists
- Sender callout
- ...

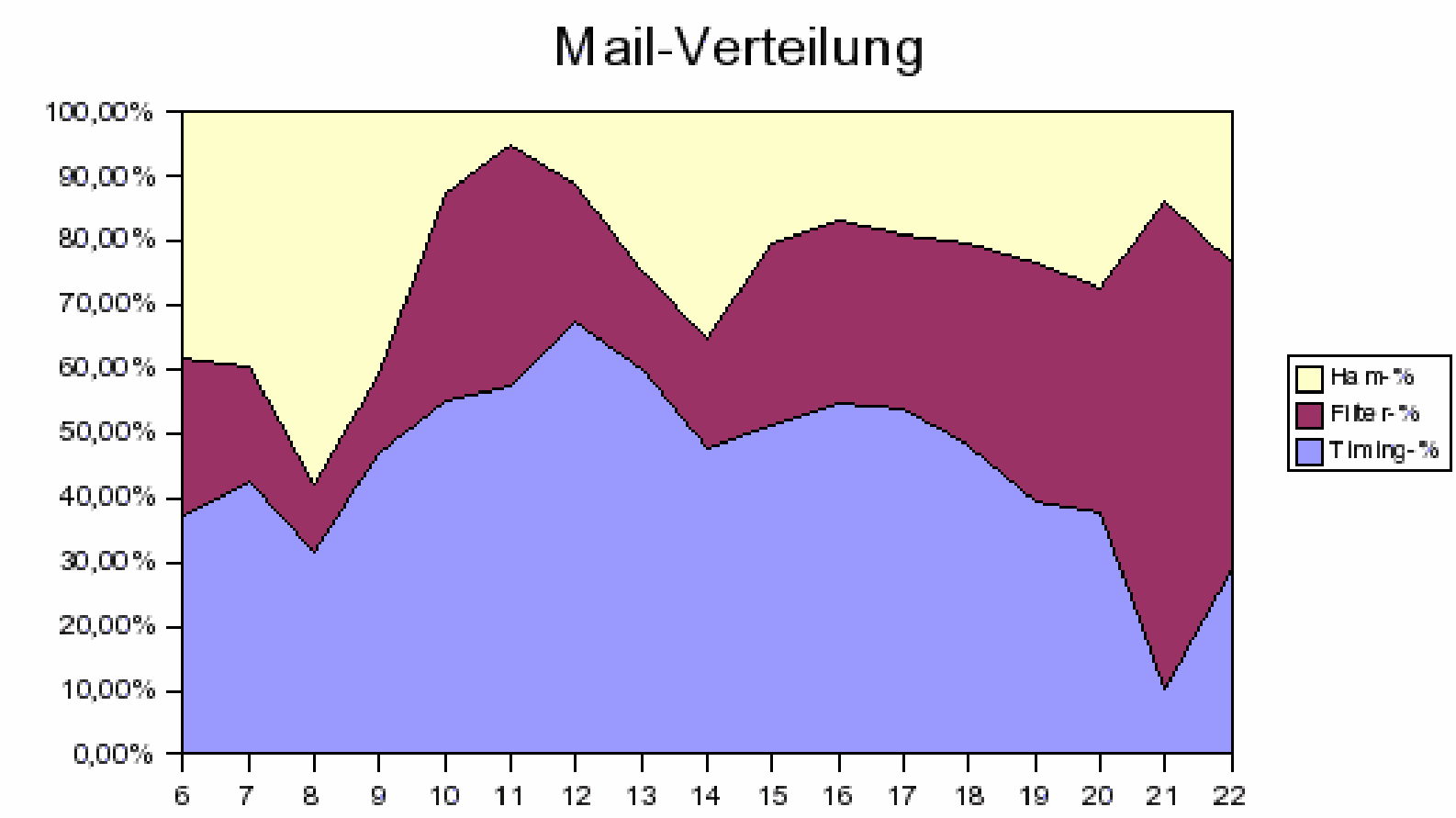
iKu Systemhaus AG

UCE: Timing-Analyse

- Spammer verwenden spezielle Software
- Viren sind fehlerhaft implementiert
- beides kann am Zeitverhalten erkannt werden
- 50-60% des Spams
- 80-90% der Viren
- Erkennung vor der Übertragung der Mail
  - weniger CPU-Last

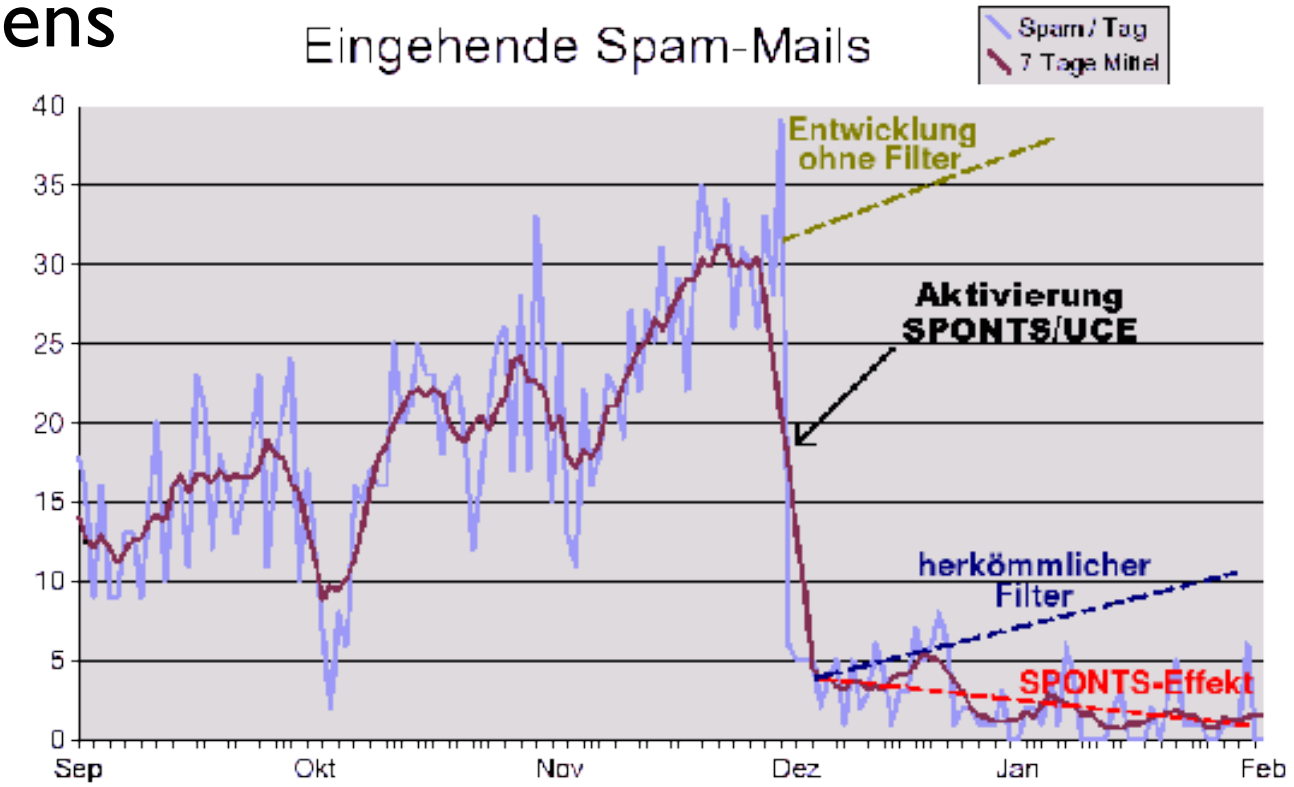
UCE: Timing-Analyse

- weniger Traffic



UCE: Verleugnung

- „Benutzer unbekannt“ auf SMTP-Ebene
- auf lange Zeit Reduzierung des Spam-Aufkommens



UMS – Unterbrechungsfreie Mailversorgung

- „POP3 auf die Warteschlange“
- 1 virtuelles Postfach
- Überbrückung von Ausfall- oder Wartezeiten

iKu Systemhaus AG

Replay

- „Online Backup“
- Speicherung der Mails im Ringpuffer
- erneutes Versenden mit einem Klick
- Replay nach bestimmten Kriterien möglich
- benutzerspezifisch

iKu Systemhaus AG

Journal

- Speicherung in SQL
- schnelle, flexible Auswertung
- einfache Integration in NOC
- alle relevanten Daten
  - Absender, Empfänger
  - Datum, Uhrzeit
  - Betreff
  - Attachments mit Dateiname und -größe

TKÜV

- Überwachung von
  - SMTP
  - POP3
  - IMAP
- Verschlüsselung
  - SSL
  - TLS

Überwachungsmaßnahme

- maximal 3 Monate
- eine Verlängerung auf 6 Monate möglich
- per Fax
  - keine Mehrwertnummern zulässig
- Einrichtung innerhalb von
  - < 10.000: 24 Stunden
  - > 10.000: 6 Stunden

Administration per Web-Interface

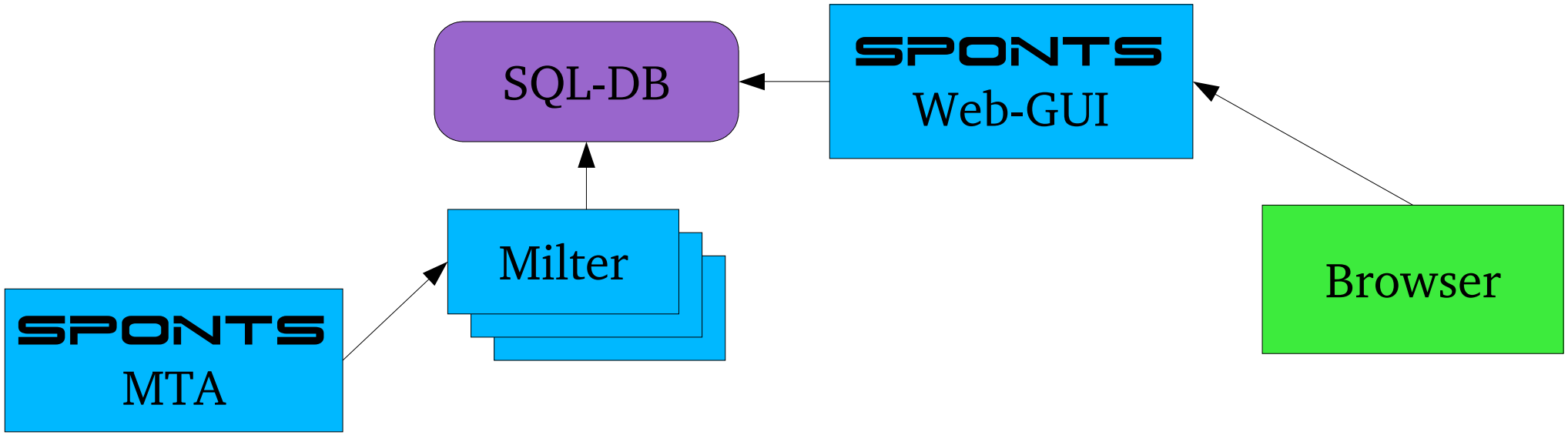
- Einrichtung einer Überwachungsmaßnahme von überall möglich
- SSL-Verschlüsselung

Administration per SOAP

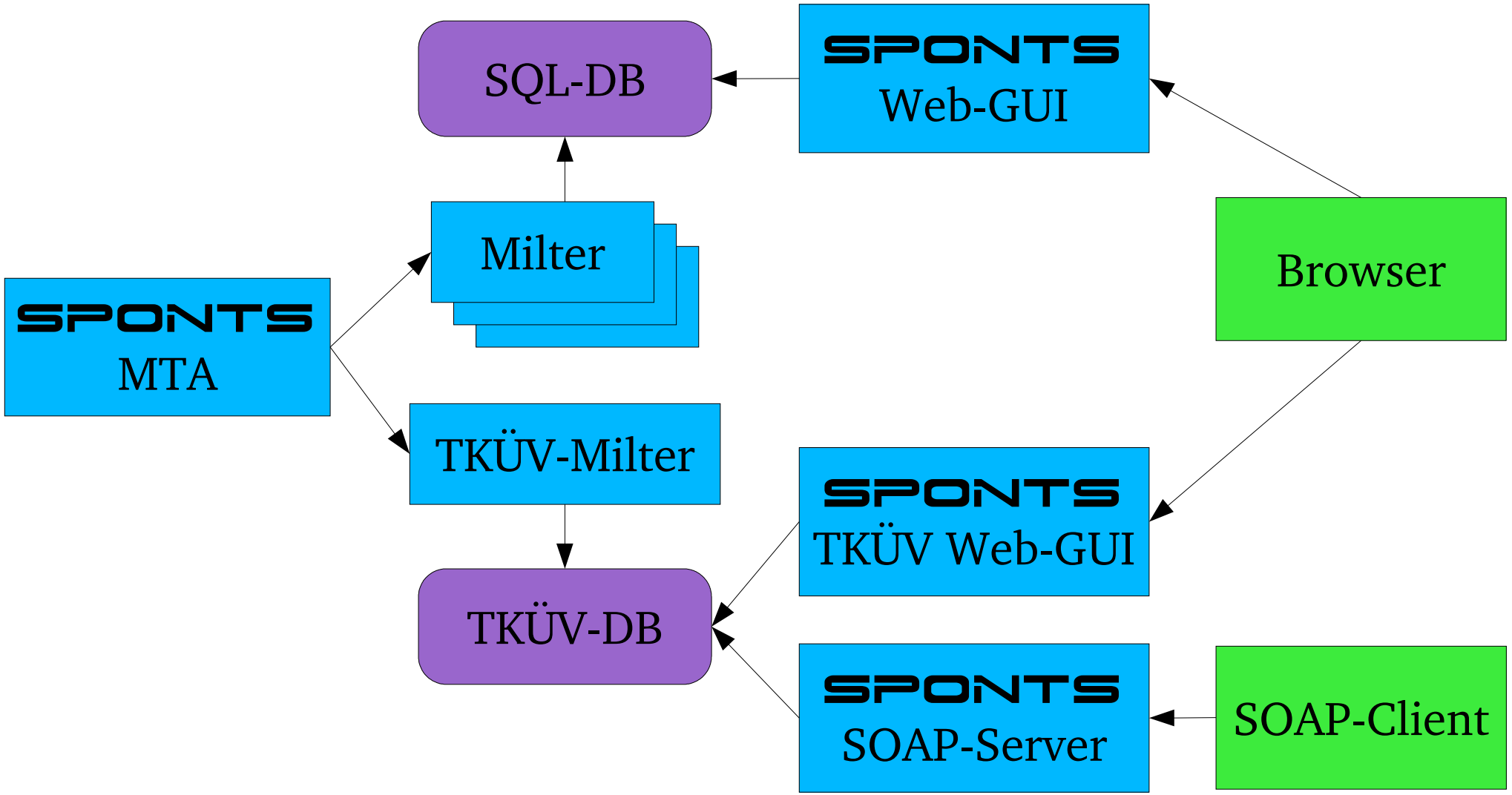
- XML über HTTP
- signiert, verschlüsselt, authentisiert
- sehr einfache Anbindung per Software
- Java
  - zwei Zeilen „Magie“
  - zwei Zeilen für Einrichtung

```
SpontsTkuev_Stub stub = (SpontsTkuev_Stub)
    new SpontsTkuev_Stub_Impl().getSpontsTkuevIFPort();
stub._setProperty(javax.xml.rpc.Stub.ENDPOINT_ADDRESS_PROPERTY,
                  System.getProperty("endpoint"));
stub.login("kurt", "*******");
stub.createMeasure("k.huwig@iku-ag.de",
                   "kurt"
```

Aufbau SPONTS

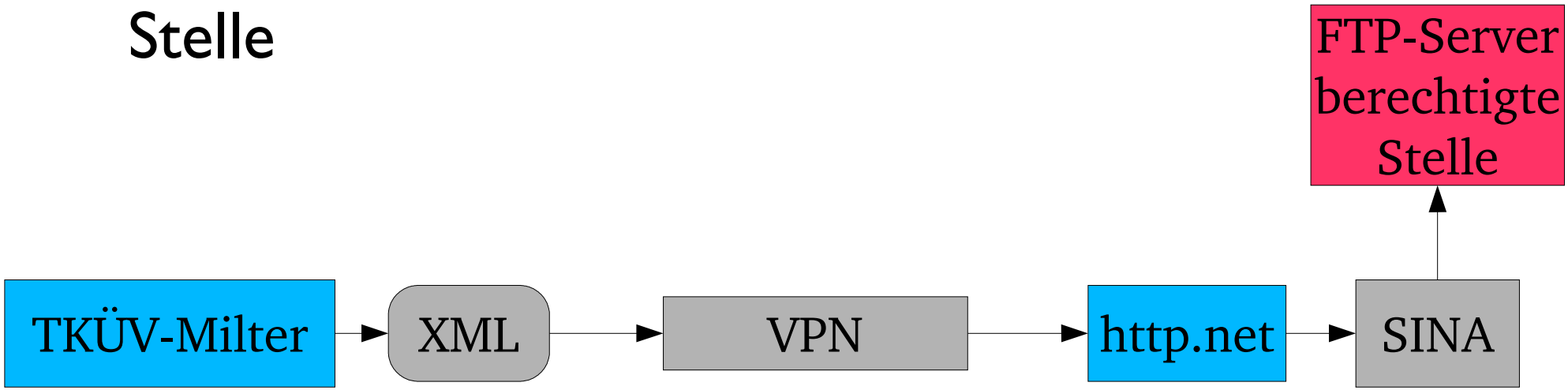


Aufbau SPONTS/Monitor



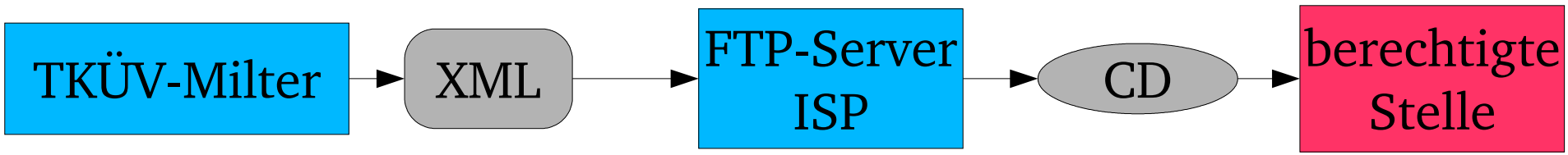
Ausleitung Ereignisdaten über SINA-Box

- VPN zu http.net
  - normales IPSec
  - SSL in Vorbereitung
- Übertragung per FTP direkt zur berechtigten Stelle



Unter 10.000 Accounts: CD mit Ereignisdaten

- geschützten FTP-Server einrichten
- an Stelle der berechtigten Stelle eintragen
- Daten auf CD brennen
- per Post an berechtigte Stelle



Einbindung von SMTP

- Store-and-Forward-Proxy
  - Backend braucht beim Verbindungsaufbau nicht bekannt zu sein
  - eine IP/Port für viele Backends
- Möglichkeiten der Einbindung
  - MX-Eintrag im DNS ändern
  - Port-Forwarder
  - IP-Adressen anpassen

Einbindung von POP3/IMAP

- Transparenter Proxy
  - Backend muss beim Verbindungsaufbau bekannt sein
  - für jedes Backend eigene IP und/oder Port
- Möglichkeiten der Einbindung
  - Port-Forwarder
  - IP-Adressen anpassen

Verhalten bei Ausfall

- eigene IP
  - Port-Forwarder auf redundantes System
- Port-Forwarder
  - Umstellen auf redundantes System
- eine Lizenz gilt für zwei redundante Systeme!

Fragen? & Antworten!
Vorführung