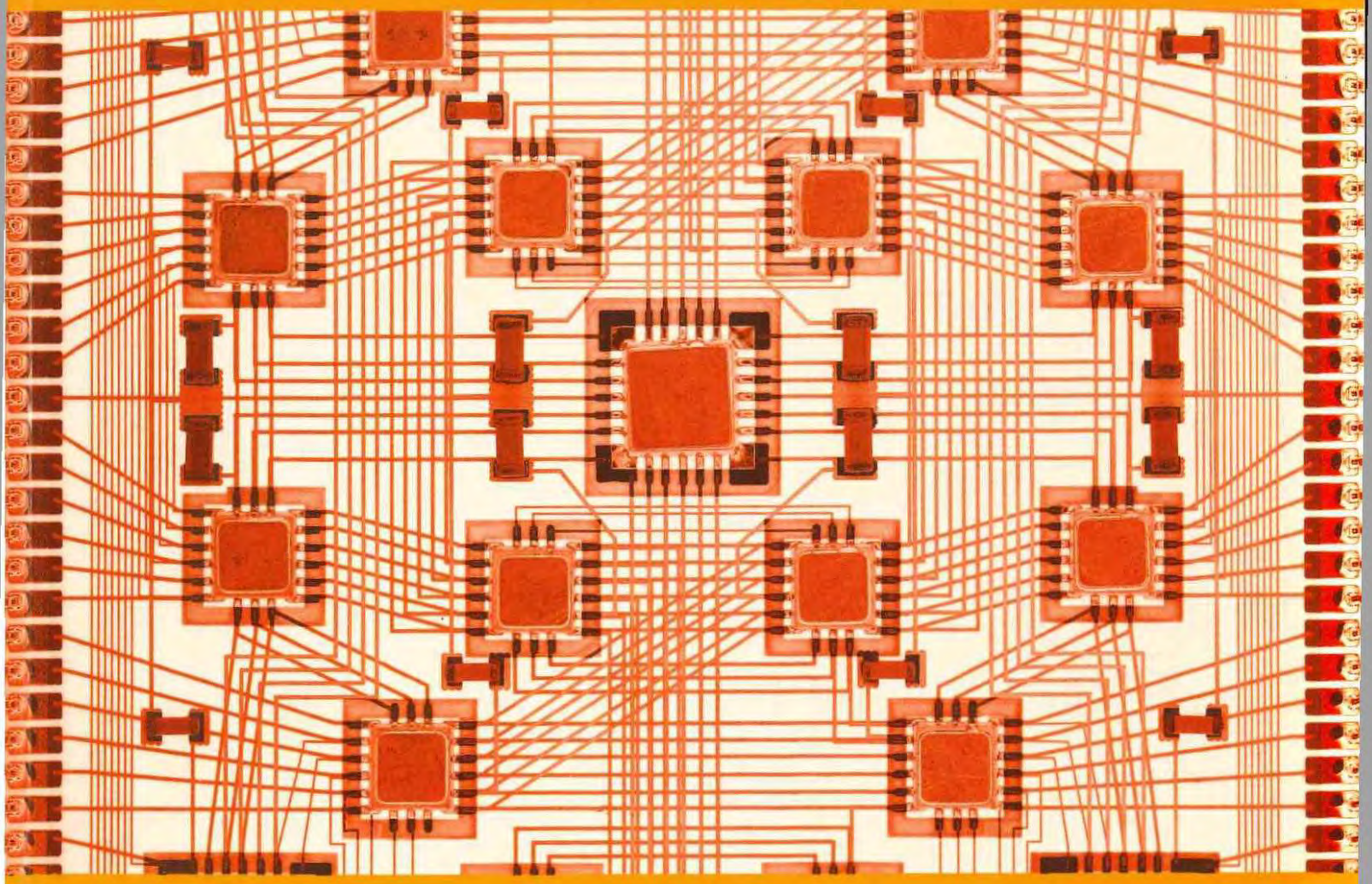
Landesamt für
Datenverarbeitung
und Statistik NRW

LDVZ - Nachrichten

1 / 2004



5. Jahrgang • Ausgabe 1 / 2004

LDVZ – Nachrichten

Herausgeber:
Landesamt
für Datenverarbeitung und Statistik
Nordrhein-Westfalen

Redaktion:
Petra Rose,
Alfons Koegel

Kontakt:
Landesamt für Datenverarbeitung
und Statistik NRW
Postfach 10 11 05
40002 Düsseldorf,
Mauerstraße 51
40476 Düsseldorf

Telefon:
0211 9449-01
Telefax:
0211 442006
Internet:
http://www.lds.nrw.de
E-Mail:
poststelle@lds.nrw.de

Auflage:
1 500

Druck:
Druckhaus Arns, Remscheid

Bestell-Nr. Z 09 1 2004 51

ISSN 1616-377X

. . . in Kürze

Schwerpunktthemen

. . . in Kürze

Geheimhaltung sensibler Daten in Veröffentlichungstabellen mit dem Quaderverfahren

Die Geheimhaltung von sensiblen Daten in zu veröffentlichenden mehrdimensionalen, d. h. nach mehreren Gliederungsmerkmalen gegliederten Statistiktabellen ist eine äußerst komplexe zeit- und personalintensive Aufgabe der amtlichen Statistik. Zur Erleichterung dieser Aufgabe hat das LDS NRW bereits Anfang der 80er-Jahre das Quaderverfahren als allgemein einsetzbares EDV-Verfahren entwickelt. Dieses Verfahren wurde bisher fortwährend an die neuesten Anforderungen angepasst.

Das Quaderverfahren schützt sensible Daten in mehrdimensionalen Statistiktabellen durch Sperren von Tabellenwerten in den Ecken mehrdimensionaler Quader. Es bietet Intervallschutz, d. h. es sichert die sensiblen Tabellenwerte so, dass ein Tabellennutzer diese Werte auch unter Zuhilfenahme von Vorwissen höchstens bis auf vorgegebene Schutzintervalle genau berechnen kann.

Unter Vorwissen wird hier das beim Tabellennutzer zu unterstellende Wissen über die Tabellenwerte verstanden, das dieser ohne Kenntnis der Tabelle haben kann. Als Quellen des Vorwissens kommen bereits veröffentlichte Tabellen in Betracht, wie z. B. zeitperiodische Veröffentlichungstabellen, so genannte Zeitreihentabellen.

Durch Berücksichtigung von Vorwissen kann man also nun auch Zeitreihentabellen zuverlässig sichern. Dabei erhalten Tabellenwerte, die in der Vorperiode offen waren, kleinere Schätzintervalle als die von gesperrten Vorperiodenwerten, weil die aktuellen Tabellenwerte aus offenen Vorperiodenwerten genauer geschätzt werden können als aus zuvor gesperrten Werten. Weil gesperrte Werte mit großen Schätzintervallen mehr Sicherheit bieten als solche mit kleinen Intervallen, übertragen sich Sperrungen in Zeitreihen oft über mehrere Perioden auf die jeweils aktuelleren Tabellenwerte. Dieses bisher eher intuitiv praktizierte „Durchstechen“ kann man jetzt Sperrungen sparender und sicherer durchführen.

Der letzte Entwicklungsstand des Quaderverfahrens wird durch das EDV-Programm QUIT repräsentiert. **QUIT** steht für **Qu**aderverfahren **it**erativ und bezeichnet den iterativen Abgleich von mehreren Statistiktabellen mit gemeinsamen Tabellenwerten zur Gewährleistung der Geheimhaltung auch solcher Werte. Unter Berücksichtigung von Vorwissen über die Tabellenwerte in Gestalt von Schätzintervallen **bietet** das Programm einen **hinreichenden Intervallschutz** für mehrfach durch Zwischensummen unterteilte Statistiktabellen und **kann** für die geheimen Werte **Schutzintervalle anstelle von Sperrvermerken ausgeben**. Es sichert simultan bis zu 20 einander überlappende Statistiktabellen, d. h. bis zu 20 Tabellen mit gemeinsamen Tabellenwerten. Das Programm eignet sich für die Sicherung von Statistiktabellen mit bis zu 100 000 Tabellenfeldern.

QUIT ist eine Weiterentwicklung des EDV-Programms **GHMITER** (Geheimhaltung iterativ), das noch mit Abgleich von zwischensummenfreien Teilen jeder einzelnen Statistiktabelle, dem sogenannten Untertabellenabgleich arbeitet und daher keine Schutzintervalle ausgeben kann. Dennoch bietet GHMITER Intervallschutz, und zwar mit Berücksichtigung von Vorwissen in Form von Schätzintervallen. GHMITER eignet sich besonders **für** die **Sicherung sehr großer Statistiktabellen** mit 1 000 000 und mehr Tabellenfeldern und wird in diesem Tabellenbereich immer ein breites Anwendungsfeld finden. Eine umfassende Beschreibung des Quaderverfahrens mit besonderem Bezug zu seinen beiden letzten Realisierungen, GHMITER und QUIT, findet man unter www.lds.nrw.de/webshop/ (Stichwortsuche: Quaderverfahren) im Webshop als PDF-Version.

Das Quaderverfahren ist als GHMITER außer im LDS NRW in mehreren Bundesländern und im Statistischen Bundesamt eingeführt. Das Statistische Amt der Europäischen Gemeinschaft (Eurostat) hat GHMITER im Rahmen des Europäischen Geheimhaltungs-Projekts CASC (Computational Aspects of Statistical Confidentiality) in das EDV-Programmpaket τ-Argus integriert. Außerdem ist – ebenfalls im Auftrage von Eurostat – von der amerikanischen Firma Anite Systems mit Subunternehmen GE-Systems in Luxemburg ein nutzerfreundliches Interface CIF (Confidentiality Interface) erstellt worden. Damit wurde GHMITER schon auf sehr umfangreiche Eurostat-Statistiken angewendet, die dadurch jetzt erstmals veröffentlicht werden konnten. Solche Tabellen waren bisher mit keinem anderen Geheimhaltungsverfahren zu bearbeiten.

Das Ende September 2003 fertiggestellte und dem LDS NRW vorgelegte EDV-Programm QUIT ist bereits als Laufzeitversion und als Quellenprogramm zusammen mit umfangreicher Beschreibung zu Methodik und Anwendung an das Statistische Bundesamt und an GE-Systems (als Eurostat-Vertretung) ausgeliefert worden. Es wird dort wie sein Vorgängerprogramm GHMITER auch in das Programmpaket τ-Argus und in das nutzerfreundliche Interface CIF eingepasst.

Dietz Repsilber
Telefon: 0211 9449-6302
E-Mail: dietz.repsilber@lds.nrw.de

DIN EN ISO 9001-Zertifizierung auf die gesamte LDVZ erweitert

Um ihren Aufgaben als IT-Kompetenz- und Dienstleistungszentrum der Landesverwaltung NRW auch in Zukunft gerecht zu werden, hatte sich die Landesdatenverarbeitungszentrale (LDVZ) im LDS NRW dazu entschlossen, ein Qualitätsmanagementsystem (QM-System) zu implementieren, das im Jahr 1999 nach der DIN EN ISO 9001:1994 zertifiziert wurde. Der Geltungsbereich des QM-Systems umfasste zunächst den Bereich der „Anwendungsbereitstellung".

In den folgenden Jahren stand die Weiterentwicklung des QM-Systems mit den nachstehend aufgeführten Schwerpunkten im Mittelpunkt:
– Sicherstellung der nachhaltigen Wirksamkeit des QM-Systems
– Ausweitung des QM-Systems auf alle Bereiche der LDVZ

Die Erteilung des Zertifikats bedeutet zunächst, dass der initiale Aufbau des QM-System erfolgreich war. „Qualität" der Prozesse und Dienste ist jedoch eine bleibende Aufgabe und unterliegt einer ständigen Weiterentwicklung. Es muss deshalb eine kontinuierliche Verbesserung erfolgen, um eine nachhaltige Wirksamkeit des QM-Systems zu gewährleisten.

Zusätzlich zu den Maßnahmen zur nachhaltigen Wirksamkeit des QM-Systems wurde bis 2002 eine sukzessive Ausweitung des QM-Systems der LDVZ auf die folgenden Bereiche vorgenommen:
– IT-Aus- und Fortbildung
– IT-Produktion
– IT-Beschaffung

Im Jahr 2002 erfolgte die erfolgreiche Rezertifizierung gemäß der revidierten und „schärferen" DIN EN ISO 9001:2000.

Nach der Einbindung der Bereiche
– IT-Infrastruktur und
– Consulting

in das QM-System wurde der Geltungsbereich des Zertifikats im Rahmen eines Überwachungs- und Erweiterungsaudits im Oktober 2003 auf die gesamte LDVZ erweitert. Das LDS NRW hat damit einen weiteren wichtigen Schritt im Rahmen der Verwaltungsmodernisierung (Binnenmodernisierung) abgeschlossen.

Mit der Ausweitung des Geltungsbereichs des Zertifikats auf die gesamte LDVZ steht bei der Weiterentwicklung die Sicherstellung der nachhaltigen Wirksamkeit des QM-Systems im Mittelpunkt der weiteren Überlegungen und Maßnahmen. Wie bereits erwähnt, erfordert nachhaltige Wirksamkeit stets einen kontinuierlichen Verbesserungs- und Optimierungsprozess. Nur so lässt sich gewährleisten, dass das QM-System auch in Zukunft effektiv, aktuell und praxisgerecht bleibt. Bei der Abwicklung dieser Prozesse wurde und wird die LDVZ von einer Vielzahl von Beschäftigten (z. B. Auditorenteam. Geschäftsprozess-Teams, Q-Team) unterstützt, die neben ihrem Tagesgeschäft freiwillig weitere Aufgaben übernommen haben. Der Erfolg ihrer Arbeit wurde wiederum durch die Erweiterung des Geltungsbereichs des Zertifikats bestätigt.

Dr. Joachim Möhring
Qualitätsmanagementbeauftragter
der LDVZ im LDS NRW
Telefon: 0211 9449-3492
E-Mail: joachim.moehring@lds.nrw.de

IT in den staatlichen Prüfungsämtern – Die Vernetzung der Schulverwaltung schreitet fort

Im Jahr 2003 beschloss das Ministerium für Schule, Jugend und Kinder NRW (MSJK) die Aufrüstung der Infrastruktur der staatlichen Prüfungsämter für erste und zweite Staatsprüfungen. Dazu gehören die Aktualisierung der Betriebssysteme auf den vorhandenen Servern und Clients, die Erneuerung veralteter Hard- und Software, die Vereinheitlichung der Systemlandschaft sowie eine Verbesserung der Netzwerkanbindung ausgesuchter Dienststellen. Das LDS NRW erhielt im Frühjahr 2003 den Auftrag, diese Umstellung zu vollziehen.

Die fünf Staatlichen Prüfungsämter I in NRW (mit jeweils mehreren Dienststellen) betreuen die Lehramtsstudent(inn)en bis nach der Absolvierung des ersten Staatsexamens. Zu den Aufgaben gehören u. a. die Verwaltung der Daten der Prüfungskandidat(inn)en, die Organisation der Prüfungen inklusive Erstellung der Prüfungspläne, Prüferbestellung, Registrierung der Noten, Zeugnisdruck sowie die Gebührenabrechnung für die Prüfer.

Die beiden staatlichen Prüfungsämter II in Düsseldorf bzw. Dortmund verwalten die Daten der Referendarinnen und Referendare in NRW während ihres zweijährigen Vorbereitungsdienstes, der mit dem zweiten Staatsexamen abgeschlossen wird. Die Aufgaben dieser Stellen umfassen die Verarbeitung von Informationen über Kandidat(inn)en und Prüfer/-innen, Notenübersichten, Hausarbeiten, das Drucken der Zeugnisse nach erfolgtem Examen, Bestellung der Zweitgutachter und Gebührenabrechnungen.

Zur Bewältigung dieser Aufgaben setzen die Prüfungsämter I und II zur Zeit verschiedene lokale Access-Anwendungen ein, die im Dezernat 235 des LDS NRW in den letzten Jahren entwickelt wurden. Der Support und notwendige Änderungen/Erweiterungen werden ebenfalls vom LDS NRW durchgeführt. Alle Prüfungsämter sind an das Landesverwaltungsnetz (LVN) angebunden und verfügten bisher über 64kB-Leitungen.

Ein Kernpunkt des eingangs beschriebenen Auftrages an das LDS NRW hinsichtlich der Modernisierung der IT-Infrastruktur bei den Prüfungsäm-

tern II ist die Umstellung der in diesen Dienststellen lokal verwendeten Access-Datenbanken auf einen zentralen SQL-Server, der im Rechenzentrum des LDS NRW betrieben wird. Das Datenaufkommen der Fachanwendungen hat insbesondere im Bereich der Prüfungsämter II zwischenzeitlich ein Volumen erreicht, das den Einsatz eines mächtigeren Datenbanksystems erfordert. Obwohl seitens des MSJK langfristig geplant ist, ein einheitliches Datenbanksystem für beide Prüfungsämterformen einzuführen, wurde aufgrund der aktuellen Dringlichkeit (und nicht zuletzt der unmittelbar zur Verfügung stehenden Finanzmittel) zunächst die Umstellung der Datenverwaltung der Prüfungsämter II verfügt. In diesem Rahmen wurde auch die Leitungskapazität zwischen den Ämtern und dem LVN von 64 kB/s auf 2 MB/s erhöht, da die existierende, herkömmliche 1-Kanal-ISDN-Leitung den zukünftigen Anforderungen nicht mehr gerecht werden kann. Seitens der Softwareanpassung an die neuen Gegebenheiten musste die Access-Anwendung insbesondere mit Rücksicht auf den anfallenden Datenverkehr zwischen Client und Server optimiert werden. Schließlich stellen auch 2 MB/s eine begrenzte Netzkapazität dar und können damit – je nach Auslastung – einen erheblichen Flaschenhals verkörpern. Daher war darauf zu achten, dass die überarbeitete PÄ II-Applikation so wenig Netzressourcen wie möglich in Anspruch nimmt, um dem Benutzer eine größtmögliche Arbeitsergonomie zu bieten.

Während diese Zeilen geschrieben werden, läuft ein umfassendes Testprogramm des neuen Systems, bestehend aus (i) einem LDS-internen Probelauf zur Prüfung der Funktionalitäten und (ii) einem Pilottest vor Ort im Prüfungsamt Düsseldorf zur Simulation der Anwendung unter realen Bedingungen. Es war geplant, dieses Testverfahren zum Beginn des Jahres 2004 abzuschließen. Bis Ende März 2004 wird dann das bestehende lokale DB-System vollständig durch die SQL-Server-Variante abgelöst.

Der unmittelbare Vorteil der Serverumstellung der Prüfungsämter II von lokalen Access-Datenbanken auf einen zentralen SQL-Server liegt darin, dass verschiedene Daten der Referendarinnen und Referendare direkt der Datenbank des Lehrereinstellungsverfahrens (LEV, ebenfalls vom LDS NRW entwickelt und betreut) innerhalb des LVN zur Weiterverarbeitung zugeführt werden können. Bisher verlief diese Übertragung über verschlüsselte E-Mails. Die Daten mussten dann vom LDS NRW manuell in die LEV-Umgebung eingepflegt werden. Darüber hinaus erhielten die Prüfungsämter II vom LDS NRW regelmäßig auf dem Postweg Disketten mit Informationen aus dem Seminareinweisungsverfahren (eine Access/SQL-Server-Anwendung, die ebenfalls vom LDS NRW entwickelt wurde und dort gehostet wird). Der Prozess des Beschreibens und Versendens der Disketten kann in Zukunft durch eine Datenübertragung auf direktem elektronischem Wege ersetzt werden.

Mittelfristig gesehen stellt diese Maßnahme nur einen ersten Schritt der vollständigen Integration aller am Lehrerausbildungs- und Einstellungsprozess beteiligten Dienststellen
- Prüfungsämter I
- Bezirksregierungen
- Studienseminare
- Prüfungsämter II

in das LVN. Dazu gehört auch die derzeit laufende Anbindung der ca. 100 Studienseminare, in welchen die Referendarinnen und Referendare in eigenen Räumlichkeiten während des Vorbereitungsdienstes durch Fachleiter/-innen betreut werden. Diese Studienseminare werden – ebenso wie die Prüfungsämter II – aus Gründen der Datensicherheit zur Zeit noch mit Informationen aus dem Seminareinweisungsverfahren über den Postversand von Disketten versorgt (ca. 100 Disketten pro Sendung). Zwischen den Studienseminaren und den Prüfungsämtern II findet ein besonders intensiver Datenaustausch statt, der zur Zeit per E-Mail, Fax und Telefon realisiert wird. Außerdem werden auf beiden Seiten unabhängig voneinander größere Datenmengen vorgehalten, die weitgehend redundant sind. Daher könnte gerade hier eine verbesserte Netzwerkinfrastruktur in Verbindung mit einer zentralisierten Datenhaltung zu einer deutlichen Erhöhung der Performance und Einsparung von Ressourcen beitragen.

Nach Abschluss der gesamten Entwicklung wird die Schulverwaltung in NRW über eine gut abgestimmte IT-Infrastruktur zur Verwaltung von Lehramtsstudent(inn)en während ihres gesamten Ausbildungsprozesses bis hin zu ihrer Einstellung als Lehrer/-in und darüber hinaus verfügen, die durch Flexibilität, kurze Wege und größtmögliche Datensicherheit charakterisiert ist.

Dr. Harald Geiger
Telefon: 0211 9449-2946
E-Mail: harald.geiger@lds.nrw.de

„IT-Hotline 4200“ – Hier werden Sie geholfen ...

LDS NRW übernimmt PC-Service für das Ministerium für Wirtschaft und Arbeit.

Seit dem 1. Januar 2004 leistet das Landesamt für Datenverarbeitung und Statistik NRW (LDS NRW) die IT-Betreuung im Ministerium für Wirt-

schaft und Arbeit (MWA) des Landes Nordrhein-Westfalen. Die entsprechende Dienstleistungsvereinbarung wurde von der Leiterin der Zentralabteilung des MWA, Frau Maria Huesmann-Kaiser, und dem Präsidenten des LDS NRW, Herrn Jochen Kehlenbach, unterzeichnet. Das MWA ist damit das erste Ministerium, das mit dem LDS NRW in diesem Segment zusammenarbeitet.

Hohe Anforderungen formulierte das MWA im vergangenen Jahr für den zukünftigen IT-Support der ca. 450 PC-Arbeitsplätze im Ministerium: „Kurze Reaktionszeiten, hohe Flexibilität, fachliche Kompetenz, Einsatz von Fernwartungssoftware und die Implementierung eines automatisierten Managementsystems für die Bearbeitung von Fehlermeldungen“ sind nur ein kleiner Auszug aus dem vom MWA vorgegebenen Pflichtenheft.

Mit dem LDS NRW hat das MWA nun einen Dienstleister beauftragt, der das Ministerium bei der Modernisierung und Optimierung seiner IT-Betreuung maßgeblich unterstützen wird.

„Die Entscheidung, das LDS NRW mit dieser Aufgabe zu betrauen, war naheliegend. Kein anderer IT-Dienstleister verfügt“ so die zuständige Abteilungsleiterin im MWA des Landes NRW, Frau Maria Huesmann-Kaiser, „über vergleichbar detaillierte Kenntnisse der IT-Infrastruktur in NRW-Behörden.“

Den Mitarbeiterinnen und Mitarbeitern im Ministerium wird zukünftig werktags durchgehend von 7.00 bis 18.00 Uhr qualifiziertes Servicepersonal für Problemlösungen und Softwareunterstützung zur Verfügung stehen.

Einen hohen Stellenwert im neu entwickelten Supportkonzept des MWA wird die telefonisch und per E-Mail erreichbare qualifizierte Servicehotline im IT-Service-Center des LDS NRW (ITSC) erhalten.

Das ITSC stattet neue Arbeitsplätze im Ministerium mit Hardware und Software aus, es berät die Mitarbeiterinnen und Mitarbeiter bei der Anwendung von Programmen und beseitigt Störungen, die im täglichen Betrieb auftreten.

Dienstleistungsvereinbarung über IT-Support im MWA durch das LDS NRW (von links: Dr. Bruno Vogel (LDS NRW), Dr. Jörg Hintelmann (LDS NRW), Präsident Jochen Kehlenbach (LDS NRW), Frau Maria Huesmann-Kaiser (MWA), Gregor Franzmann (MWA))

Mit Hilfe des im LDS NRW gebündelten Fachwissens und dem Einsatz des modernen Fernwartungswerkzeugs Microsoft SMS 2003 sollen Probleme der Anwenderinnen und Anwender zukünftig noch zeitnäher gelöst und der kostenträchtige „Turnschuh“-Support deutlich reduziert werden.

Allerdings müssen die zu betreuenden Mitarbeiterinnen und Mitarbeiter im MWA nicht auf den gewohnten „Vor-ort-Service“ verzichten; denn diverse Problemlösungen (z. B. Hardwaredefekte) lassen sich nur direkt am Arbeitsplatz erledigen. Mit den vereinbarten kurzen Reaktionszeiten wird das neue Supportmodell dem Anspruch einer möglichst unterbrechungsfreien Verfügbarkeit der PC-Arbeitsplätze gerecht und leistet so einen wichtigen Beitrag zu Effizienzsteigerung im Ministerium.

Weitere Synergieeffekte liegen in der Nutzung der zentralen Hardwarebeschaffung durch das LDS NRW und des im ITSC vorhandenen Know-hows für größere IT Projekte wie z. B. Betriebssystem-Migrationen oder die Einführung neuer Softwareversionen.

Mittelfristig rechnen MWA und LDS NRW sogar mit einer noch weitergehenden Effizienzsteigerung, da über das neu eingesetzte Trouble-Ticket-System nicht nur Supportanfragen erfasst und systematisch abgearbeitet werden können, sondern auch aussagekräftige Daten für ein effektives IT-Controlling erhoben werden. Häufig auftretende technische Schwachstellen können so zuverlässig identifiziert und bei zukünftigen Problemlösungen oder Beschaffungen berücksichtigt werden.

Mit dem ITSC hat das LDS NRW seine Angebotspalette um ein zunehmend nachgefragtes Produkt erweitert. „Wir sind uns bewusst“, konstatierte Präsident Kehlenbach bei der Unterzeichnung der Vereinbarung, „dass nur die von uns angestrebte hohe Qualität der Dienstleistung und eine maximale Zufriedenheit unserer Auftragsgeber Grundlage für die Gewinnung weiterer Kunden in diesem Segment sein werden.“

Gregor Franzmann (MWA)
Telefon: 0211 8618-4348
E-Mail: gregor.franzmann@mwa.nrw.de

Dr. Jörg Hintelmann (LDS NRW)
Telefon: 0211 9449-2424
E-Mail: joerg.hintelmann@lds.nrw.de

SPAM
– und (k)ein Ende?

Ein Artikel in den LDVZ-Nachrichten 2/2003 hat sich mit den grundsätzlichen Aspekten von Spam beschäftigt. Als Nachtrag und Fortsetzung geht es in diesem kurzen Bericht um die praktischen Erfahrungen mit Spam und dessen Bekämpfung im Landesverwaltungsnetz.

„Du kommst hier nicht 'rein!“

Mit diesem Satz machte ein großer Internet-Service-Provider auf seinen verbesserten Schutz vor Spam aufmerksam.

Am Eingang zum Landesverwaltungsnetz einen „Türsteher“ zu postieren, der unerwünschte „Gäste“ (Absender von Nachrichten) abweist, ist zumindest technisch nicht besonders aufwendig. Hier ist eine Liste von Adressen zu pflegen, die bei der Übertragung nicht zugelassen werden.

Das Problem lag auch weniger im technischen Umfeld als im Adressbestand, der von den betroffenen Empfängern zur Verfügung gestellt wurde. Denn die verbreitete Eindeutschung des Begriffes „Spam“ als „unerwünschte Nachricht“ führte zu seltsamen Reaktionen:

– „Das Postfach hat eine Größenbeschränkung erreicht“, aber soll man deshalb eine Adresse vom Typ „postmaster @behoerde.nrw.de“ wirklich sperren?
– Man hat vielleicht vergessen, wie man sich von einer Mailing-Liste abmeldet. Aber die Sperrung der Adresse hätte vielleicht Auswirkungen auf 100 andere Empfänger im Land, die auf die Information für ihre Arbeit angewiesen sind.
– Hat man eine Viren-Warnung bekommen, so sollte man den Absender nicht gleich auf die „schwarze Liste“ setzen. Der Schutz vor Viren wird im Landesverwaltungsnetz groß geschrieben, sodass im Regelfall wirklich nur eine Warnmeldung erzeugt wird. Aber soll man den Urheber auf Dauer von jeglicher Kommunikation ausschließen?

Wenn sich unter diesen Umständen die Pflege der Adressliste schon als etwas aufwändiger herausstellte, so war das erzielte Ergebnis nicht dazu angetan, auch nur einen Hauch von Begeisterung hervor zu rufen.

Von mehr als 1 500 Adressen tauchten vielleicht einmal 3 Prozent wieder auf mit der Bemerkung „Regel führt zur Unterbindung der Übertragung“.

Ein Blick auf typische Absender-Adressen zeigt auch: Aus „fr54q@yahoo.com“ kann morgen sehr schnell „fr45q@yahoo.com“ werden. Einerseits wechseln Spammer Ihre Absender-Adresse schneller als ein Chamäleon die Farbe, andererseits ist zu beobachten, dass Spammer immer häufiger echte Adressen „ausleihen“. So setzen sie auch modifizierte Schadenssoftware wie Viren oder Trojaner, die sich selbst nicht mehr verbreiten, sondern einmalig auf dem Wirt-System die Nachricht an alle Adressen im lokalen Adressbuch versenden.

Wirksame(re) Mittel und Wege

Da das Sperren von Absender-Adressen keinen nennenswerten Erfolg zeigte, war die Suche nach besseren Werkzeugen erforderlich.

Die Hersteller von Antiviren-Software bieten Erweiterungen, die auch zur Bekämpfung von Spam eingesetzt werden können.

Allerdings erwiesen sich diese Produkte als relativ starr in der Administration und lieferten in einem Testbetrieb eine Vielzahl von nicht erklärlichen „falsch positiven“ Ergebnissen. Die Einstellungen „Weiterleiten“, „Blockieren“ und „Löschen“ als Ergebnis einer Analyse sind in einem homogenen Firmennetzwerk als hinreichend zu betrachten (schließlich ist das Löschen von Nachrichten ein Eingriff in den elektronischen Postverkehr und bedarf einer Betriebsvereinbarung), für das Landesverwaltungsnetz mit seinen vielen unabhängigen Einrichtungen ist der Einsatz solch eines Produktes allerdings nicht so einfach zu befürworten.

Deshalb war der testweise Betrieb eines Spam-Analyse-Tools auf der Basis von „SpamAssassin“ weniger eine Entscheidung für eine kostengünstige (die Software ist als Open-Source-Produkt kostenfrei), als vielmehr für eine flexible, anpassungsfähige Lösung, die den unterschiedlichsten Bedürfnissen gerecht werden kann.

SpamAssassin analysiert eine Nachricht nach unterschiedlichen Kriterien und vergibt für das Auftreten bestimmter Merkmale Punkte, die zu einem Gesamtergebnis addiert werden. Die Anzahl der Treffer ist dann eine Maßzahl für die Spam-Wahrscheinlichkeit der Nachricht. So werden auch Probleme mit der einfachen Mustererkennung umgangen: „V.I-A.G-R.A“ im Betreff ist für den Menschen immer noch lesbar, einige Programme steigen hier aber aus, da die Liste der „verbotenen Wörter“ dieses phantasievolle Konstrukt nicht enthält.

Die ersten (derzeit auch noch aktuellen) Einstellungen sahen für die Einordnung als Spam eine Punktzahl von 5, für das Blockieren der Nachricht eine Punktzahl von 12 vor. Erkannte Nachrichten werden in veränderter Form weiter geleitet, indem sie als Anhang in eine neue Nachricht eingebettet werden. Zustellbestätigungen oder Abwesenheitsnotizen an einen gegebenenfalls überhaupt nicht existierenden Absender werden so vermieden. Der beim Öffnen einer Nachricht teilweise unumgängliche Verbindungsaufbau in das Internet ebenfalls.

Seit Anfang Oktober 2003 wurden die Nachrichten an das LDS NRW dieser Überprüfung unterzogen. Glücklicherweise konnten auch noch andere Einrichtungen der Landesverwaltung für den Testbetrieb gewonnen werden bzw. einige andere Einrichtungen haben sich mit der Bitte um Einbeziehung in den Testbetrieb gemeldet.

Ein Zeitraum von nunmehr fast drei Monaten sollte für eine erste Bestandsaufnahme hinreichend sein:
Unabhängig von der Zahl der einbezogenen Adressaten liegt der Anteil von erkannten Spam-Nachrichten bei ungefähr 10 Prozent. 1 bis 2 Prozent erreichen den zweiten Schwellwert von 12 und werden auf dem Analyse-System blockiert. In diesem Fall erhält der Empfänger einmal täglich eine Benachrichtigung mit den wichtigen Details der eingegangenen Nachrichten.

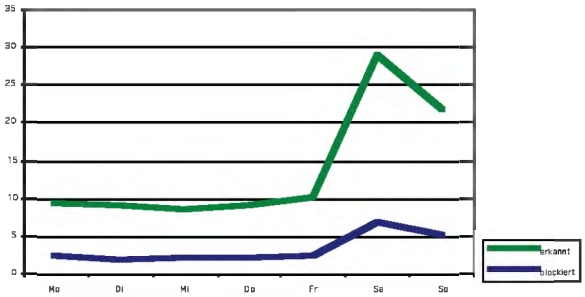
Das Zahlenmaterial erlaubt auch einen ersten Überblick über den Spam-Anteil am gesamten Nachrichtenverkehr. Die folgenden Grafiken zeigen den prozentualen Anteil über eine durchschnittliche Woche beziehungsweise Tag.

Diese Zahlen sagen allerdings noch nichts über die Qualität der Analyse aus. Deshalb hier einige Bemerkungen zu den gemachten Erfahrungen.

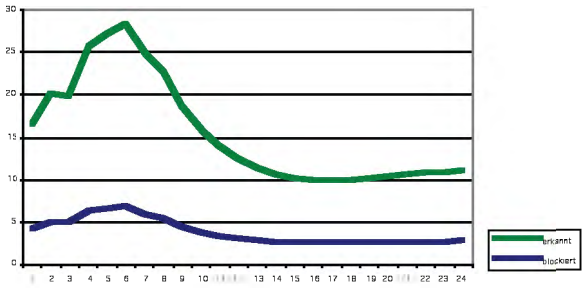
Es gab immer noch einen Anteil von eindeutig als Spam eingestuften Nachrichten, die in der Bewertung unter den erforderlichen Punkten blieben.

Vereinzelt kam es zu einer Bewertung als Spam, die sich als nicht gerechtfertigt erwies. In diesem Fall gibt es aber Einstellungsmöglichkeiten, die es gestatten, bezogen auf den Empfänger das Ergebnis um 6, 20 oder 100, bezogen auf den Absender das Ergebnis um 100 Punkte zu verringern. Somit kann die automatische Bearbeitung von Nachrichten, die an der „Weiterleitung“ der ursprünglichen Mitteilung scheiterte, sicher gestellt werden.

SPAM-Anteil in Prozent (Wochenübersicht)



SPAM-Anteil in Prozent (Tagesübersicht)



Es hat sich aber im Laufe der Zeit heraus gestellt, dass das System „lernfähig“ ist. Im Hintergrund läuft ein ständiger Prozess, der aus der Analyse Merkmale gewinnt, die in eine „Wahrscheinlichkeit“ münden.

Die Regel „Spam-Wahrscheinlichkeit nach Bayes-Test xx %“ gelangt immer häufiger zum Einsatz und hat die Qualität der Erkennung erheblich verbessert.

Es gibt auch die Möglichkeit, diesen Lernprozess mit entsprechenden Nachrichten anzustoßen. Allerdings verändern viele Systeme in der Landesverwaltung bei der Weiterleitung Nachrichten in einer Form, dass sie für den Einsatz nicht mehr in Frage kommen.

Ausblick

Es mag seltsam klingen, aber: Je mehr Spam, desto besser die Analyse.

Daher kann man von der Erweiterung der Testumgebung oder von einem nahezu flächendeckenden Einsatz einiges erwarten.

Die Reduktion des Gesamtaufkommens wäre sicherlich wünschenswert, aber an erster Stelle steht vorläufig die Verminderung der Belästigung der Anwender.

Die Erkenntnisse der nächsten Zeit können durchaus Auswirkungen auf die Server-Topologie im Bereich der E-Mail-Kommunikation haben.

Unter Umständen erhält man auch Hinweise auf besonders auffällige IP-Adressen, die im normalen Nachrichtenaustausch nicht in Erscheinung treten, sich aber als Spam-Plattform auszeichnen.

Sie können davon ausgehen, dass auch in Zukunft die Entwicklung des Systems, des Marktes – vielleicht kommt ja doch noch die ultimative Lösung – und des rechtlichen Umfeldes genauestens beobachtet wird.

Gerold Vannahme
Telefon: 0211 9449-3380
E-Mail: gerold.vannahme@lds.nrw.de

Open Source Software auf Webservern im LDS NRW

Freie Software und mehr noch *Open Source* haben sich auch im Bereich der öffentlichen Verwaltung zu Schlagworten entwickelt.

Wörtlich übersetzt bedeutet der Begriff „Open Source“ offene Quelle. Das bedeutet nicht nur, dass die Software frei und uneingeschränkt genutzt werden darf, sondern darüber hinaus auch vom Anwender modifiziert werden kann. Der Begriff Open Source entstand 1998 auf einer Entwicklerkonferenz in Palo Alto, Kalifornien. Damit sollte verdeutlicht werden, dass Open Source mehr ist als nur frei erhältliche, kostenlose Software.

Eine genaue Definition was Open Source Software ist, wird durch die Open Source Initiative herausgegeben und ist weitgehend anerkannt:

Die Definition quelloffener Software (“Open Source Software”)
Version 1.9

Einführung
“Quelloffen” (“open source”) bedeutet nicht nur freien Zugang zum Quellcode. Bei quelloffener Software müssen die Lizenzbestimmungen in Bezug auf die Weitergabe der Software folgenden Kriterien entsprechen:

1. Freie Weitergabe
Die Lizenz darf niemanden in seinem Recht einschränken, die Software als Teil eines Software-Paketes, das Programme unterschiedlichen Ursprungs enthält, zu verschenken oder zu verkaufen. Die Lizenz darf für den Fall eines solchen Verkaufs keine Lizenz- oder sonstigen Gebühren festschreiben.

2. Quellcode
Das Programm muss den Quellcode beinhalten. Die Weitergabe muss sowohl für den Quellcode als auch für die kompilierte Form zulässig sein. Wenn das Programm in irgendeiner Form ohne Quellcode weitergegeben wird, so muss es eine allgemein bekannte Möglichkeit geben, den Quellcode zum Selbstkostenpreis zu bekommen, vorzugsweise als gebührenfreien Download aus dem Internet. Der Quellcode soll die Form eines Programms sein, die ein Programmierer vorzugsweise bearbeitet. Absichtlich unverständlich geschriebener Quellcode ist daher nicht zulässig. Zwischenformen des Codes, so wie sie etwa ein Präprozessor oder ein Konverter (“Translator”) erzeugt, sind unzulässig.

3. Abgeleitete Software
Die Lizenz muss Veränderungen und Derivate zulassen. Außerdem muss sie es zulassen, dass die solcherart entstandenen Programme unter denselben Lizenzbestimmungen weitervertrieben werden können wie die Ausgangssoftware.

4. Unversehrtheit des Quellcodes des Autors
Die Lizenz darf die Möglichkeit, den Quellcode in veränderter Form weiterzugeben, nur dann einschränken, wenn sie vorsieht, dass zusammen mit dem Quellcode so genannte “Patch files” weitergegeben werden dürfen, die den Programmcode bei der Kompilierung verändern. Die Lizenz muss die Weitergabe von Software, die aus verändertem Quellcode entstanden ist, ausdrücklich erlauben. Die Lizenz kann verlangen, dass die abgeleiteten Programme einen anderen Namen oder eine andere Versionsnummer als die Ausgangssoftware tragen.

5. Keine Diskriminierung von Personen oder Gruppen
Die Lizenz darf niemanden benachteiligen.

6. Keine Einschränkungen bezüglich des Einsatzfeldes
Die Lizenz darf niemanden daran hindern, das Programm in einem bestimmten Bereich einzusetzen. Beispielsweise darf sie den Einsatz des Programms in einem Geschäft oder in der Genforschung nicht ausschließen.

7. Weitergabe der Lizenz
Die Rechte an einem Programm müssen auf alle Personen übergehen, die diese Software erhalten, ohne dass für diese die Notwendigkeit bestünde, eine eigene, zusätzliche Lizenz zu erwerben.

8. Die Lizenz darf nicht auf ein bestimmtes Produktpaket beschränkt sein
Die Rechte an dem Programm dürfen nicht davon abhängig sein, ob das Programm Teil eines bestimmten Software-Paketes ist. Wenn das Programm aus dem Paket herausgenommen und im Rahmen der zu diesem Programm gehörenden Lizenz benutzt oder weitergegeben wird, so sollen alle Personen, die dieses Programm dann erhalten, alle Rechte daran haben, die auch in Verbindung mit dem ursprünglichen Software-Paket gewährt wurden.

9. Die Lizenz darf die Weitergabe zusammen mit anderer Software nicht einschränken
Die Lizenz darf keine Einschränkungen enthalten bezüglich anderer Software, die zusammen mit der lizenzierten Software weitergegeben wird. So darf die Lizenz z. B. nicht verlangen, dass alle anderen Programme, die auf dem gleichen Medium weitergegeben werden, auch quelloffen sein müssen.

Quelle: http://www.telcor.gob.ni/BCS/nd/Open Source.org/docs/osd-german.html

Herausragendes Merkmal von Open Source Software ist das Lizenzmodell unter dem die Software steht. Hierbei existieren mehrere Lizenzausgestaltungen, die diesen Tatbestand erfüllen.

Die wohl am häufigsten genutzte Open Source Lizenz ist die GNU GPL (GNU General Public License). Merkmal dieser Lizenzform ist, dass Kopieren und Modifizieren der Software erlaubt ist, aber die modifizierte Software ebenfalls wieder der GPL unterstellt sein muss. Dadurch wird sichergestellt, dass ein Programmcode, der von seinen Entwicklern als quelloffen gedacht ist, nicht mit geringen Änderungen versehen und dann wieder geheim gehalten wird. [http://www.gnu.de/gpl-ger.html] Die älteste und ebenfalls weit verbreitete Form ist die BSD-Lizenz. Solange die ursprünglichen Copyright-Vermerke erhalten bleiben, ist jede Form der Weitergabe freigestellt. Sie stammt von der Universität von Berkley, wobei BSD für Berkley Software Distribution steht. [http://www.de.freebsd.org/copyright/license.html]

Die Einsatzmöglichkeiten von Open Source Software sind breit gefächert. So werden bereits seit 1996 Webserver des LDS NRW unter dem Betriebssystem Linux und dem Webserver Apache betrieben. Zur Zeit werden circa 500 Webangebote von Behörden und Einrichtungen des Landes NRW unter Linux/Apache gehostet. Darauf aufbauend wird eine große Anzahl an Open Source Produkten auf den Webservern eingesetzt, die hier ebenfalls aufgeführt und beschrieben werden sollen.

Linux ist ein frei verfügbares Unix-Betriebssystem, das ursprünglich 1991 von dem finnischen Studenten Linus B. Torvalds entwickelt wurde. Linux unterliegt der GNU GPL und ist damit frei verfügbar. Diese freie Verfügbarkeit hat dazu geführt, dass Entwickler auf der ganzen Welt an diesem Betriebssystem mitarbeiten und damit die Entstehung einer leistungsfähigen und stabilen Plattform vorangetrieben haben und permanent weiterentwickeln. Linux wird in der Regel in Form von Distributionen vertrieben, wobei dazu Pakete aus dem Linux-Kernel und diverser Software zusammengestellt werden. Die Entwicklung von Installationsroutinen, das Zusammenstellen von Konfigurationsprogrammen, die Produktion der Installationsmedien sowie die Erstellung von gedruckten Handbücher bedingen die Preise von Distributionen. Die bekanntesten Distributionen sind SuSE, Red Hat, Debian und Mandrake. Erwähnenswert ist hier, dass Debian die einzige Linux-Distribution ist, die ausschließlich aus Open Source Produkten besteht.

Ein sicher ebenso bekanntes Open Source Projekt ist der **Apache** Webserver. Release 1.0 wurde 1995 veröffentlicht. Er bietet eine Vielzahl an Konfigurationsmöglichkeiten und zeichnet sich durch gute Performance aus. Weiterhin bietet er eine große Bandbreite an Modulen für die verschiedensten Zwecke (PHP, PERL, SSL...). Der Apache ist weltweit der verbreitetste Webserver und besitzt einen Anteil von fast 70 %, wie die Netcraft Statistik zeigt (Abb. 1):

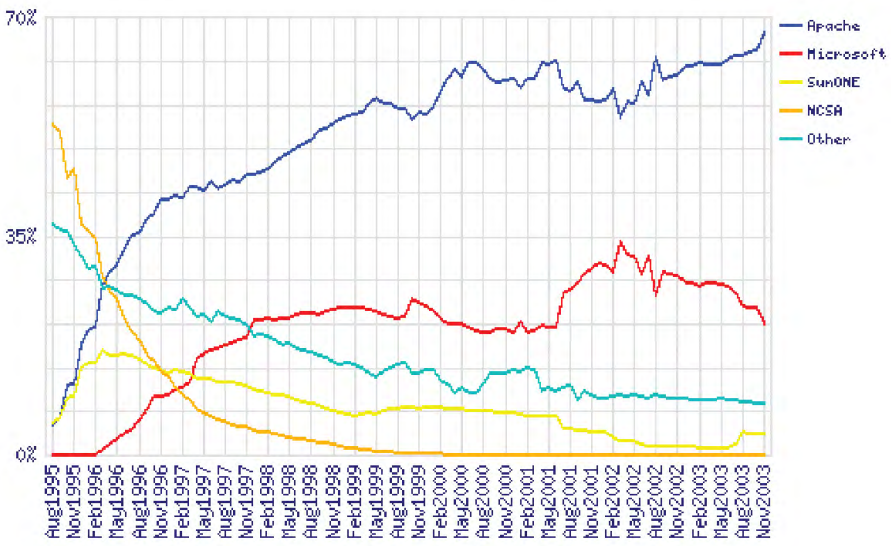


Abb. 1: Quelle: http://news.netcraft.com/archives/2003/11/index.html

MySQL ist eine bekannte und gebräuchliche Open Source Datenbank, die 1996 der Öffentlichkeit vorgestellt wurde. Seitdem erfreut sie sich bei Linux-Anwender sowie Webdesignern größter Beliebtheit. Auch die Features des Datenbanksystems werden stetig weiterentwickelt. Unter den Kunden des LDS NRW werden innerhalb der Webangebote häufig MySQL Datenbanken eingesetzt, so dass die Datenbank-Systeme mittlerweile auf eigenen Servern laufen (je einer für Inter- und Intranet).

PHP ist eine populäre Open Source Skriptsprache speziell für Web-entwicklungen und lässt sich in HTML einbinden. Ein wichtiger Aspekt dieser Sprache ist es, Webentwicklern die Möglichkeit zu geben, schnell dynamisch generierte Webseiten zu erzeugen. Eine große Stärke von PHP ist die Unterstützung von Datenbankabfragen, es bietet sich so die Möglichkeit der einfachen Erstellung von datenbankgestützten Webseiten.

Die Kombination der vier oben beschriebenen Softwareprodukte wird häufig als **LAMP** bezeichnet, einem Akronym für Linux, Apache, MySQL und PHP.

Die erste Version der Programmiersprache **Perl** (Practical Extraction and Report Language) wurde 1987 durch Larry Wall veröffentlicht. Hauptziel war es, mit Perl eine Skriptsprache zu entwickeln, die es ermöglichen sollte, Textdateien komfortabel zu bearbeiten. Im Laufe der Zeit wurde das CPAN (Comprehensive Perl Archive Network) geschaffen, ein Onlineverzeichnis für Perl-Quellcode, Dokumentationen, Skripte sowie Module und Erweiterungen. Hier wird die Kooperation innerhalb der Open Source-Community besonders deutlich. Mittlerweile ist Perl zu einer der wichtigsten Programmiersprachen für Systemadministration und Webprogrammierung geworden.

Um mittels serverseitiger Java-Programme dynamische Webangebote und Webapplikationen realisieren zu können, werden sowohl Java Servlets als auch JavaServer Pages (JSP) eingesetzt. Bei beiden handelt es sich um Java-Komponenten, die von einem Java-basierenden Webserver unterstützt werden müssen. Dazu wird im LDS NRW die Software **Tomcat** auf einigen Webservern eingesetzt.

Tomcat ist ein Open Source-Container für Java-basierte Web-Anwendungen, der Servlet- und JSP-Web-Anwendungen ausführt. Er wird als offizielle Referenzimplementierung für die Servlet- und JSP-Spezifikationen von der Apache Software Foundation unter dem Projektnamen "Jakarta" entwickelt.

Für Bretter und Foren des LDS NRW, die täglich mehr als 20.000 Zugriffe verzeichnen, wird die Software **phpbb** eingesetzt. Diese basiert wiederum auf den Open Source Produkten PHP und MySQL. Die phpBB-Community stellt laufend neue Templates und Module bereit, mit denen die phpBB-Foren indi-vidualisiert werden können. Auch die Vielzahl an Features, die diese Anwendung bietet, ist bemerkenswert, hier seien exemplarisch die Möglichkeiten der Foren-administration, Benutzer- und Gruppenverwaltung sowie die Moderationsmöglichkeiten genannt.

Für die Auswertung von Webserver-Logfiles zum Erstellen von Webstatistiken sind auf den LDS-Webservern die Open Source Tools Webalizer und Analog im Einsatz:

Der **Webalizer** ist ein Programm zur Darstellung von Zugriffsstatistiken einer Webseite (Abb. 2). Die Auswertungsmöglichkeiten sind recht umfangreich und lassen sich über die Konfigurationsdatei des Webalizers und des Webservers einrichten.

Auch die Software **Analog** ermöglicht die Aufbereitung und Darstellung von Zugriffsstatistiken. Auch hier lassen sich die Reports und Grafiken umfassend konfigurieren (Abb. 3).

Der auf einem Webserver des LDS NRW eingesetzte **MapServer** ist ein Tool, das die Möglichkeit der Navigation in Karten bietet. Er verarbeitet etliche der in diesem Bereich verwendeten Standardformate (GIS, ESRI) zur Beschreibung von Karten (Abb. 4). Auch die Ausgabe lässt sich in Standardfor-

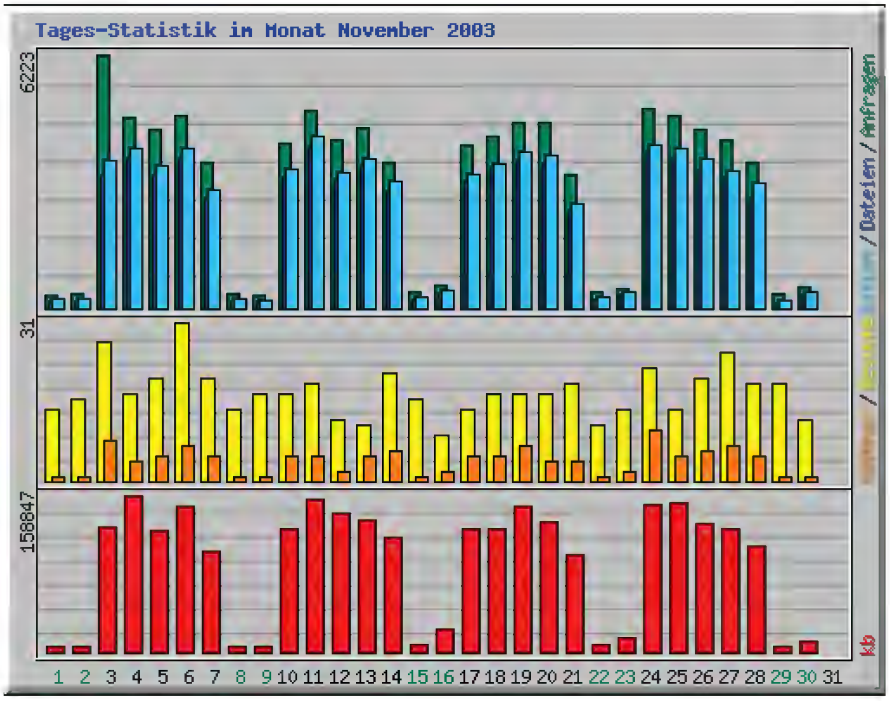


Abb. 2: Beispiel einer Webalizer-Grafik

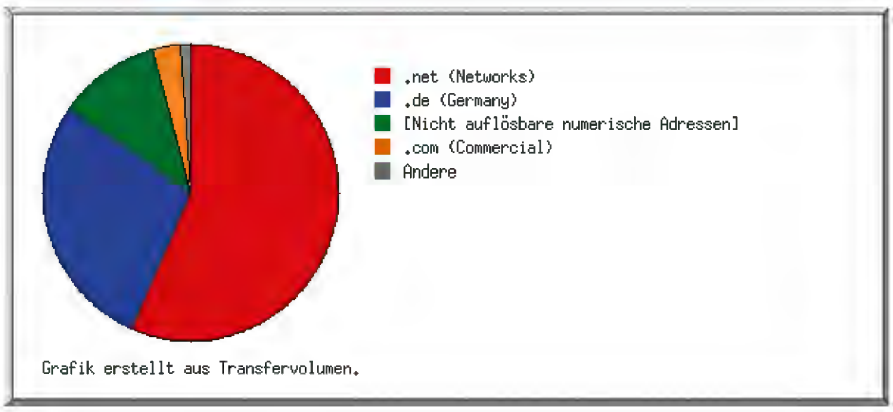


Abb. 3: Beispiel einer Analog-Grafik

maten konfigurieren (TIFF/GeoTIFF, GIF, PNG, ERDAS, JPEG). Die Grundlage dieses Systems ist der University of Minnesota MapServer, eine Entwicklung der University of Minnesota.

Für die Zukunft ist eine weitere Ausdehnung der Verwendung von Open Source Software geplant. So sollen für einen Kunden des LDS NRW ein Shop- und ein Auktionssystem eingerichtet werden. Hierzu werden zur Zeit die Produkte OS-Commerce und webauction getestet.

Die erweiterte Markupsprache XML (eXtensible Markup Language) ist ein vom World-Wide-Web-Konsortium (W3C) vorgeschlagener Dokumentenverarbeitungsstandard. Es wird erwartet, dass XML und die gesamte Familie der XML-Technologien zum Standard für die einheitliche Speicherung von Daten wird. Das Grundkonzept von XML ist die Trennung von Inhalt, Struktur und Layout in separaten Dateien. Durch diese Trennung wird ein plattformunabhängiger Datenaustausch möglich.

Für zukünftige Webangebote bedeutet dies, dass Webseiten mit viel und einheitlich strukturiertem Inhalt, die Daten immer häufiger in XML-basierten, eigenen Dateiformaten speichern. Für die Darstellung solcher Dokumente im Browser existieren bereits serverseitige Open Source Tools, die die benötigten Transformationen vornehmen können. Hier sei das ebenfalls von der Apache Software Foundation initiierte Cocoon-Projekt erwähnt.

Der Einsatz von Open Source bietet einige Vorteile. Zunächst ist hervorzuheben, dass für die Produkte keine Lizenzkosten anfallen und die Software

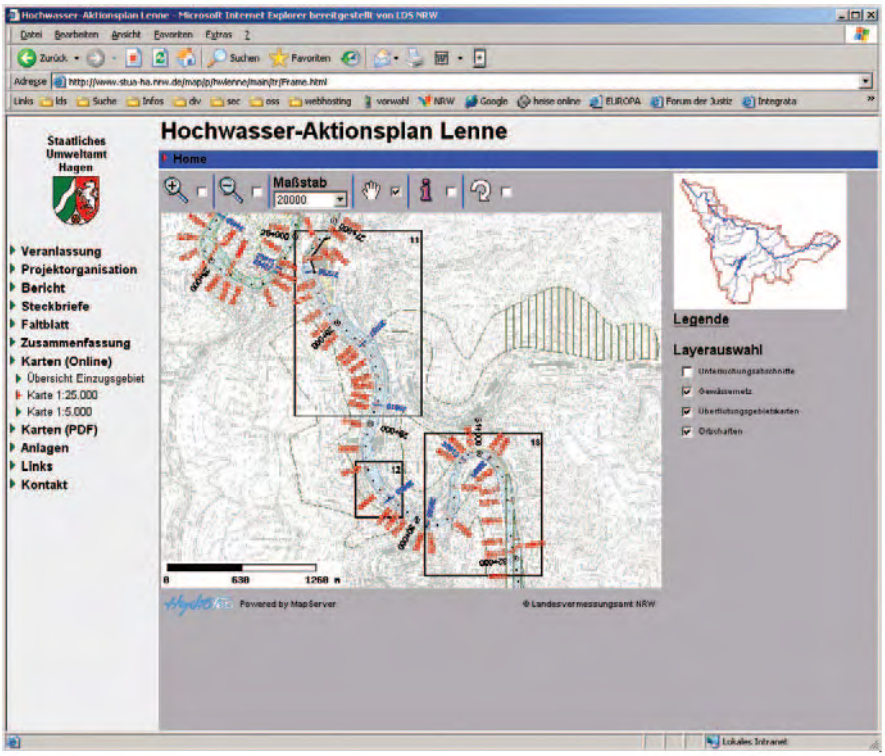


Abb. 4: Beispielseite unter Verwendung des Mapservers

beliebig oft installiert werden kann. Auch Updates und Upgrades können kostenlos bezogen werden.

Durch die Verfügbarkeit des Quelltextes entfällt auch die Abhängigkeit von nur einem Hersteller. Für Support und Weiterentwicklung können die geeignetsten Dienstleister ausgewählt werden. Zusätzlich bietet die freie Verfügbarkeit auch die Möglichkeit die Software an die eigenen Anforderungen anzupassen und individuell zu erweitern. Die Vielzahl der Entwickler sorgt für eine stetige Weiterentwicklung der Software und die schnelle Fehlerbeseitigung. Dies ist insbesondere in sicherheitskritischen Bereichen von Vorteil, da auf diesem Weg auch Sicherheitslücken schnell geschlossen werden können. Da insbesondere Webserver durch das Internet öffentlich zugängliche Systeme sind, ist hier der Sicherheitsaspekt besonders wichtig.

Mit dem Einsatz sowohl von Open Source Software als auch proprietärer Software und den damit gewonnenen Erfahrungen hat das LDS NRW die Voraussetzungen dafür geschaffen, auch in Zukunft den Einrichtungen und Behörden des Landes NRW als kompetenter Berater zur Verfügung zu stehen.

Genauere Informationen, u. a. über erforderliche organisatorische Schritte und fachkundige Gesprächspartnerinnen und -partner zu allgemeinen Fragen oder zu individuellen Fachthemen werden gerne vom LVN-Nutzerservice (Tel. 0211 9449-2350, Fax 0211 9449-8350, E-Mail: lvn-nutzerservice@lds.nrw.de) vermittelt.

Susanne Schmitz
Telefon: 0211 9449-2060
E-Mail: susanne.schmitz@lds.nrw.de

Gefahren durch Viren

Die Anzahl der Computerviren, die heute auf die PC-Anwenderinnen und -Anwender losgelassen werden, steigt von Jahr zu Jahr an. Auch die Tricks, mit denen die Programmierer solcher Computerviren arbeiten, um einen Computer zu infizieren, werden immer besser und ausgefeilter: Sei es die Ausnutzung von Sicherheitslücken oder auch das Design einer virenverseuchten E-Mail, das die Anwenderin bzw. den Anwender dazu verleiten soll, die Anlage in dieser E-Mail zu öffnen.

Allerdings sind auch wir als Anwender/-in von PC-Systemen oder Administratoren von Servern nicht schutzlos den Computerviren ausgeliefert. Hier gibt es Virenschutzprogramme, Firewalls und andere technische Maßnahmen, die uns vor den Viren schützen können. Und manchmal sollte uns auch der gesunde Menschenverstand helfen, den neuesten Virus nicht einfach unbedacht aus einer E-Mail heraus auszuführen.

Obwohl in der Presse und auch in diesem Artikel immer von Computerviren die Rede ist, handelt es sich bei den aktuellen Schädlingen meistens nicht um Viren, sondern um Würmer. Der Unterschied liegt eigentlich nur in der Tatsache, dass ein Computervirus, wie ein organischer Virus auch, einen Wirt braucht um sich verbreiten zu können. Der organische Virus befällt die menschlichen Zellen, um sich zu verbreiten, und der Computervirus hängt sich an ein anderes Programm an. Ein Wurm dagegen ist ein eigenständiges Programm, das sich z. B. per E-Mail verbreitet. Der Einfachheit halber werde aber auch ich bei der allgemein üblichen Bezeichnung Computervirus bleiben.

Im letzten Jahr hat es mehrere große Virenepidemien gegeben, von denen ich hier einmal exemplarisch drei Spezielle etwas genauer unter die Lupe nehmen möchte, um zu zeigen, wie sich Viren verbreiten, aber auch wie man sich vor den Viren schützen kann.

Der Virus SoBig.F

Als ersten Virus möchte ich gleich den aufführen, der sich im Jahr 2003 am besten verbreiten konnte: den Virus SoBig.F.

Hierbei handelte es sich um den 6. Virus einer ganzen Reihe von SoBig Viren, der sich hauptsächlich per E-Mail verbreitete. Es war eine Funktion eingebaut, die es ihm erlauben sollte, sich zusätzlich über freigegebene Netzwerklaufwerke zu verbreiten, diese Funktion war aber fehlerhaft programmiert, so dass dieser Weg nicht funktionierte.

Die Anwenderin bzw. der Anwender bekam den Virus in einer E-Mail, die in Englisch verfasst war. Durch Doppelklick auf die darin enthaltene Anlage wurde der Virus aktiviert. Warum konnte sich dieser Virus dann aber so gut – nicht nur im englischen Sprachraum – verbreiten?

Zum einen benutzte der Virus eine recht kurze und einfache englische Betreffzeile (z. B. „Thank you“ oder „Your Details“) und einen eben solchen Nachrichtentext (z. B. „See the attached file for details“), der auch den nicht Englisch sprechende(n) Anwender/-in dazu aufforderte, die angehängte Datei (z. B. „your_document.pif“ oder „document_ 9446.pif“) auszuführen.

Als Zweites machte sich der Virus, wie viele andere Viren auch, zunutze, dass in Windows standardmäßig bekannte Dateierweiterungen ausgeblendet werden. Die Anwenderin bzw. der Anwender bekommt also nicht „your_document.pif“ sondern nur „your_document“ zu sehen. So sieht die Anwenderin bzw. der Anwender nicht, dass es sich dabei um eine potenziell gefährliche Datei handelt.

Als Drittes, und das ist es wohl auch, was diesen Virus auf Platz 1 in allen Virenstatistiken im Jahr 2003 gebracht hat, ist die überaus effektive Methode der Verbreitung zu nennen. Konnte der Virus ein System infizieren, sammelte er erst einmal alle auf der Festplatte gespeicherten E-Mail-Adressen ein. Wenn dann eine bestehende Internetverbindung entdeckt wurde, schickte sich der Virus selbsttätig an alle diese gesammelten Adressen. Hierbei wurden Techniken benutzt, die sonst eigentlich nur beim Versenden von unerwünschten Werbe-E-Mails, so genannten SPAM-Mails, angewendet werden. Bisherige Viren schickten immer eine Kopie nach der anderen an die gesammelten Adressen. Der Virus SoBig.F schickte mehrere Kopien parallel auf einmal, wodurch eine sehr schnelle Verbreitung gelang, so dass die Antivirenhersteller noch keine Virenscanner zur Verfügung stellen konnten und viele Behörden, Firmen und Anwenderinnen und Anwender anfangs völlig ungeschützt vor dem Virus waren. Auch waren am Anfang noch keine Informationen über den Virus verfügbar, um die Anwenderinnen und Anwender zu warnen.

Der Schaden, den dieser Virus verursachte, lag daher auch nicht in einem eingebauten Schadensteil, sondern einfach in der massenhaften Verbreitung. Das E-Mail-Aufkommen war so groß, dass Netzwerkleitungen überlastet waren, E-Mail-Server die E-Mails nicht mehr abarbeiten konnten und Virenscanner den Ansturm kaum noch bewältigen konnten.

Zum Glück hatte dieser Virus ein eingebautes Verfallsdatum nach dem er nicht mehr aktiv war. Sonst wäre der Virus SoBig.F sehr viel länger ein Problem gewesen.

Der Virus Blaster (bzw. Lovesan)

Als zweiten Virus möchte ich einen ganz anderen Typ nennen, der 2003 in aller Munde war: der Virus Blaster (oder auch Lovesan).

Dieser Virus verbreitet sich nicht über E-Mail, wie es so viele andere tun, sondern versucht Windows-Computer direkt über eine Netzwerkverbindung zu infizieren.

Der Virus nutzt eine bekannte Sicherheitslücke von Windows 2000 und Windows XP im RPC Dienst aus (RPC steht für Remote Procedure Call und ist eine Methode, mit der sich Windows Rechner untereinander verständigen.).

Dabei läuft eine Infektion folgendermaßen ab:
Zuerst bekommt der Computer, der infiziert werden soll, über das Netz ein Datenpaket mit einem Teil des Virus darin zugeschickt. Dieses Datenpaket wird von dem RPC-Dienst entgegengenommen und weiter verarbeitet. Dabei wird ein Teil dieses Datenpaketes in einen bestimmten Speicherbereich geschrieben. Dieser Speicherbereich ist aber eigentlich für die Daten zu klein, so dass auch der folgende Speicherbereich überschrieben wird (Das nennt man einen Pufferüberlauf.).

Diese Daten, mit denen der folgende Speicherbereich überschrieben wurde, beinhalten genau den Virus, der an dieser Stelle dann von Windows ausgeführt wird. Dieser Teil des Virus sorgt dafür, dass der restliche Viruscode von dem System, das ihn gerade infiziert hat, heruntergeladen und auf der Festplatte gespeichert wird.

Jetzt kann dieser Computer weitere Computer, die er per Netzwerk erreichen kann, infizieren.

Als Schadensfunktion versucht der Virus eine Attacke auf die Internet-Updateseite von Microsoft auszuführen.

Der beschriebene Virus ist im Internet immer noch aktiv. Und das, obwohl für die Sicherheitslücke, die der Virus ausnutzt, schon ca. vier Wochen vor Erscheinen des Virus ein Sicherheitspatch von Microsoft zur Verfügung gestellt wurde.

Der Virus Swen.A

Als dritten und letzten Virus möchte ich den Virus Swen.A aufführen, als Beispiel dafür, wie ein Virus verschiedenste Methoden der Verbreitung benutzen kann.

Zuerst einmal verbreitete sich der Virus Swen.A per E-Mail. Dazu benutzt er eine E-Mail, die so aussieht, als würde sie von Microsoft kommen. Die E-Mail ist genau so aufgebaut, wie die Update-Seite von Microsoft im Internet und enthält angeblich einen Patch gegen eine Sicherheitslücke. Klickt die Anwenderin bzw. der Anwender, die/der diese E-Mail erhält, jetzt auf die angehängte Datei, wird ihr/ihm vorgespielt, dass sich der Sicherheitspatch installiert. In Wirklichkeit installiert sich aber im Hintergrund der Virus.

Der Virus ist aber nicht in jedem Fall auf ein manuelles Starten durch die Anwenderin bzw. den Anwender angewiesen, er kann auch eine Sicherheitslücke im Internet Explorer ausnutzen, bei der eine angehängte Datei automatisch gestartet wird, wenn man sich die E-Mail in Outlook oder Outlook Express nur anschaut.

Als zweite Methode der Verbreitung kopiert sich der Virus auf freigegebene Netzwerklaufwerke, und zwar genau in die Autostart-Ordner, die Windows beim Starten abarbeitet.

Als dritte Methode postet sich der Virus selbst in Newsgroups, wieder in der Aufmachung der Microsoft-Seite, um einen Leser der Newsgroup zum Ausführen des Anhangs zu bringen.

Viertens (und fünftens) sendet sich der Virus in IRC Chat Chanels oder stellt sich selbst zum Download über P2P-Tauschnetze (z. B. Kazaa) zur Verfügung. Dafür generiert er eine Datei, die den Virus enthält, mit einem Dateinamen, der eine Anwenderin bzw. einen Anwender dazu bringen soll, die Datei zu laden und zu öffnen (z. B. „Windows Media Player installer“, „Sobig removal tool“ oder auch „HardPorn“).

Zusätzlich versucht der Virus noch seine eigene Entdeckung zu verhindern, indem er alle laufenden Programme, die ein Virenscanner sein könnten, beendet.

Der Schaden, den der Virus anrichtet, liegt darin, dass er versucht, die Zugangsdaten der Anwenderin bzw. des Anwenders zu seinem E-Mail-Postfach in Erfahrung zu bringen. Dazu zeigt der Virus nach einiger Zeit ein Fenster, in dem erklärt wird, es habe Probleme beim Abholen von neuen E-Mails gegeben, und in dem die Anwenderin bzw. der Anwender aufgefordert wird, die Zugangsdaten inkl. Passwort zu seinem E-Mail-Postfach neu einzutragen.

Auch dieser Virus ist, obwohl schon Ende September 2003 entdeckt, im Internet noch recht aktiv unterwegs.

Was kann man gegen Viren tun?

Nach den ganzen Beschreibungen der Viren und der Methoden, wie sich die Viren verbreiten, fragt man sich, was man gegen diese Virenflut unternehmen kann. Hier gibt es natürlich einiges, was sie als Anwenderin und Anwender selbst tun können (auch an ihrem heimischen PC) und was ihr Administrator für Sie tun kann.

An erster Stelle ist hier natürlich die Anti-Viren Software zu nennen, die auf jedem Arbeitsplatz und zusätzlich auf den E-Mail-Servern, Fileservern und allen weiteren Servern, auf denen Viren abgelegt werden können oder über die sie verbreitet werden, installiert sein sollte. Diese schützt vor allen bekannten Viren. Mindestens genau so wichtig, wie eine Anti-Viren-Software auf dem System ist es aber auch, diese aktuell zu halten. Eine Anti-Viren-Software, die die neuesten Viren nicht erkennt, kann doppelt gefährlich sein, da sie nicht nur Viren ungehindert durchlässt, sondern die Anwenderin bzw. den Anwender auch in einer falschen Sicherheit wiegt, die ihn unvorsichtig werden lassen kann. Das Landesamt für Datenverarbeitung und Statistik NRW betreibt am zentralen E-Mail-Übergang vom Internet zum Landesverwaltungsnetz eine Virenscannerlösung, bestehend aus zwei unabhängigen Virenscannern. Hier wurden im letzten Jahr fast 500 000 Viren aus E-Mails entfernt (allein über 400 000 Mal der Virus SoBig.F).

Zum Schutz vor Viren wie dem Blaster sollte man sich nie ohne Firewall im Internet bewegen. Sei es die Firewall, die das komplette Behördennetz vom Internet trennt oder die persönliche Firewall, die auf dem privaten PC mit direktem Internetzugang installiert sein sollte.

Der Virus Blaster oder auch der Virus Swen.A hat bekannte Sicherheitslücken ausgenutzt um sich zu verbreiten. Hier ist es wichtig, auch bei den angebotenen Sicherheitspatches auf dem aktuellen Stand zu bleiben. Spätestens, wenn eine Sicherheitslücke in der Tagespresse erwähnt wird oder auf der Startseite des Softwareherstellers zu finden ist, sollte diese auf jedem System installiert werden.

Vor vielen Viren kann man allerdings durch einen vorsichtigen Umgang mit dem Computer verschont bleiben. Man sollte bei keiner E-Mail unbedacht eine angehängte Datei ausführen. Selbst wenn die E-Mail von einem Kollegen zu kommen scheint, sollte man vorsichtig sein, da viele Viren inzwischen die Absenderadresse in der E-Mail fälschen. Im Zweifelsfall sollte man sich evtl. vor der Ausführung einer Anlage mit dem Absender in Verbindung setzen, um zu klären, um was es sich bei der Anlage genau handelt.

Und wenn doch ein Virus auf dem Computer ist?

Durch die oben genannten Maßnahmen kann die Gefahr eines Virenbefalls sehr stark minimiert werden. Ganz ausschließen kann man aber auch bei der größten Vorsicht einen Virenbefall nie. Falls sich doch mal ein Virus auf Ihrem Computer eingenistet haben sollte, heißt die erste Regel: Keine Panik!

Oft richtet man durch überstürzte Reinigungsaktionen mehr Schaden an, als der Virus alleine hätte verursachen können.

Dann sollte der befallene Computer, wenn möglich erst einmal vom Netz getrennt werden bzw. ausgeschaltet werden. Von einem anderen Computer aus kann man dann im Internet bei den großen Anti-Viren Herstellern (z. B. unter http://www.trendmicro.de oder unter http://www.nai.com) anhand der Symptome den Virus versuchen ausfindig zu machen, der das System befallen hat. Hat man einmal den Virus identifiziert, steht meist bei der Beschreibung des Virus auch eine Anleitung, wie der Virus entfernt werden kann bzw. wird direkt ein kleines Tool zum Download angeboten, mit dem der Virus automatisch entfernt werden kann.

Zusätzlich findet man im Intranet der Landesverwaltung (http://lv.nrw.de) unter dem Punkt „Übergreifende Informationen“ weiterführende Informationen zu Computerviren allgemein. Unter dem Punkt „Aktuelles – Betriebsstörungen im LVN“ finden sich Warnungen vor Computerviren, die aktuell eine Gefahr für das Landesverwaltungsnetz darstellen.

Kai Hesse
Telefon: 0211 9449-2028
E-Mail: kai.hesse@lds.nrw.de

OBELIX und die Systemtechnik

Das LDS NRW als IT-Dienstleister der Landesverwaltung NRW entwickelt im Projekt OBELIX (OBELIX = Online Bezügeverfahren des Landes Nordrhein-Westfalen mit internen und externen Ressourcen) derzeit gemeinsam mit dem Landesamt für Besoldung und Versorgung (LBV NRW) und externen Partnern ein neues IT-Verfahren für die Zahlung der Bezüge der nordrhein-westfälischen Landesbediensteten.

Im Rahmen dieses Projektes beschreibt das LBV NRW in einem fachlichen Feinkonzept zunächst die funktionalen Anforderungen an das zu realisierende Verfahren. Darüber hinaus muss OBELIX nichtfunktionale Anforderungen erfüllen, die das LBV NRW gemeinsam mit dem LDS NRW formuliert. Gerade die nichtfunktionalen Anforderungen führen zu Architekturentscheidungen, die deutliche Auswirkungen auf das gewählte Design und die eingesetzte Systemtechnik haben.

Nichtfunktionale Anforderungen an OBELIX
- plattformunabhängiges Frontend
- Performance
- Datensicherheit und Katastrophenschutz
- Datenschutz und Revisionssicherheit
- Skalierbarkeit
- Hochverfügbarkeit

Plattformunabhängiges Frontend – Web-Technologie

Das heutige Bezügeverfahren setzt seit Jahren auf die bewährte 3270-Mainframetechnologie, obwohl die Geschwindigkeit der technischen Entwicklung stetig ansteigt und heute der PC am Arbeitsplatz der meisten Bezügebearbeiterinnen und -arbeiter dominiert. Dass eine Prognose über die IT-Entwicklungen in den kommenden Jahren sehr schwierig ist, zeigen allein in diesem Bereich die Diskussionen über die Vor- und Nachteile von Microsoft- bzw. Open-Source-Software (Linux anstelle von Windows, OpenOffice statt Microsoft Office ...).

Für das Projekt OBELIX ist zu beachten, dass die Bezügebearbeiterinnen und -bearbeiter des LBV NRW auf der einen Seite von den Vorzügen der „neuen“ Technologie profitieren sollen, auf der anderen Seite soll sich aber die gewohnte Bearbeitungsgeschwindigkeit gegenüber der heutigen 3270-terminalbasierten Großrechnertechnologie nicht deutlich verschlechtern. Antwortzeiten im Sekundenbereich, wie in 3270-Anwendungen üblich, stellen für Web-Applikationen eine echte Herausforderung dar.

Datensicherheit und Katastrophenfallvorsorge

Im Bezügeverfahren des Landes Nordrhein-Westfalen werden die Daten von ca. 600 000 Landesbediensteten gespeichert und verarbeitet. Neben den monatlichen Bezügezahlungen werden auch einmalige Zahlungen wie Abschläge, Vorschüsse, Beihilfe etc. veranlasst. Datenverluste würden sich in diesen personenbezogenen Buchungsabläufen äußerst negativ auswirken. Daher wird dieser Anforderung, Datenverluste unbedingt zu verhindern, mit umfangreichen technischen Sicherungsmaßnahmen Rechnung getragen, die in den folgenden Abschnitten dargestellt werden sollen.

Datenschutz und Revisionssicherheit

Die Sicherheit der Daten im Hinblick auf Integrität und Unversehrtheit sowie der Schutz gegen unbefugte Veränderungen wird durch das Datenschutzgesetz NRW vorgeschrieben. Ausgefeilte Berechtigungs- und Zugangskonzepte, die den unbefugten Zugang zu den personenbezogenen Daten verhindern, sowie Möglichkeiten für die Innenrevision, missbräuchlichen Datenänderungen auf die Spur zu kommen, sind beim Projekt OBELIX unbedingt erforderlich.

Skalierbarkeit

Derzeit arbeiten im LBV NRW ca. 800 Mitarbeiterinnen und Mitarbeiter mit der heutigen Bezügesoftware. Mittelfristig werden also ca. 800 User Zugriff auf OBELIX haben.

Zukünftig ist im Rahmen moderner eGovernment-Überlegungen geplant, dem Bezügeempfänger selbst über das Internet die Möglichkeit zu geben, Auskunfts- und auch bestimmte Bearbeitungsvorgänge zu tätigen. Angedacht sind hier beispielsweise der Zugriff auf elektronisch vorgehaltene Bezügemitteilungen oder die direkte Eingabe von Anschriftenänderungen. In diesem Falle läge die potentielle User-Zahl bei ca. 600 000.

Auch diese erst zukünftig zu berücksichtigende Anforderung bezüglich der Skalierbarkeit des Verfahrens beeinflusst die Systemarchitektur sowie die eingesetzte Technik.

Hochverfügbarkeit

Bei 800 Sachbearbeiterinnen und Sachbearbeitern im LBV NRW bedeutet ein Ausfall des Systems eine erhebliche Beeinträchtigung des Geschäftsbetriebs. Daher ist eine hohe Verfügbarkeit nicht nur der Anwendung, sondern auch des gesamten IT-Systems eine nichtfunktionale Anforderung von besonders hoher Priorität.

In den folgenden Abschnitten werden bei OBELIX eingesetzte Technologien, die eine besonders hohe Verfügbarkeit (24x7, zero-downtime) gewährleisten sollen, ausführlich dargestellt.

Ganzheitlicher Service

Das LBV NRW erwartet von der Landesdatenverarbeitungszentrale (LDVZ) im LDS NRW ein IT-Verfahren für die Bezügebe- und -verarbeitung. Dies umfasst neben der eigentlichen Softwareentwicklung auch die zukünftige Wartung und Pflege. Zu der ebenfalls geforderten Durchführung der Produktion gehören Rechenzentrumsleistungen, wie die Bereitstellung der Hardware und der erforderlichen Systemsoftware, Maßnahmen zur Datensicherung und Katastrophenfallvorsorge und die eigentliche Überwachung und Steuerung der Produktion, sowie Netzwerkleistungen wie der Betrieb des GON.

Die oben dargestellten nichtfunktionalen Anforderungen an das IT-Verfahren führen zu einer Reihe von Architekturentscheidungen, die sich wiederum in allen anderen Aspekten des IT-Services auswirken, z. B. in der Bereitstellung von Systemsoftware und in der Steuerung und Überwachung des Verfahrens.

Das LDS NRW setzt Systemsoftware ein, die aus heutiger Sicht eine strategische Ausrichtung auf das WEB-Geschäft hat. Dies betrifft u. a. die Software „Websphere Applikation Server“ (WAS), die im Rahmen ihrer Weiterentwicklung Services für „business to business“ Integration zur Verfügung stellt. Die nächste, bereits angedachte Entwicklungsstufe zeigt sich bereits, jetzt: die dynamische Anpassung an gestellte Anforderungen, bekannt unter dem Namen „on Demand“. Die Definition dieses neuen eBusiness-Begriffes lautet „Optimierung der Prozesse (Operations), dynamische Reaktion (Response) auf die Anforderungen der Kunden, Mitarbeiter und Partner“ (Zitat: Vortrag von Roland Trauner, IBM, 7/2003). Die WAS und die anderen durch das LDS NRW eingesetzten Softwareprodukte wie CICS, DB2 usw. stützen diesen Gedanken und werden ihn in den kommenden Releasen und Versionen immer stärker Rechnung tragen.

Im Folgenden sollen nun die verschiedenen in der Architektur von OBELIX vorgesehenen systemtechnischen Komponenten und ihr Bezug zu den nichtfunktionalen Anforderungen dargestellt werden.

OBELIX-Architektur

Eine der nichtfunktionalen Kernanforderungen an OBELIX ist das plattform- und betriebssystemunabhängige Frontend. Relativ frühzeitig im Projektverlauf fiel die Entscheidung daher für eine browserbasierte Benutzeroberfläche.

Das Land NRW hat mehr als 600 000 Zahlfälle – in der freien Wirtschaft entspricht dies den Arbeitsverträgen –, deren bezügerelevanten Daten von OBELIX verwaltet werden müssen. Im LBV entstehen dadurch große Datenmengen und hohe Transaktionsraten, so dass sich das LBV NRW sehr früh dazu entschloss, die Datenhaltung und Produktion von OBELIX auf dem IBM-Großrechnersystem der LDVZ im LDS NRW durchzuführen.

In OBELIX wird eine Web-Anwendung mit klassischer 3-Ebenen-Architektur realisiert.

3-Schichten-Architektur (three-tier)
- Schicht 1 Präsentationsebene (Browser) LBV NRW
- Schicht 2 Geschäftslogikebene (OBELIX-Programme) LDS NRW
- Schicht 3 Datenhaltungsebene (OBELIX-Datenbank) LDS NRW

Die Präsentationsschicht ist auf dem LBV-Großrechner angesiedelt, die Geschäftslogik und die Datenhaltung auf dem LDS-Großrechner. Der LDS-Rechner besteht physisch aus zwei Maschinen, die an verschiedenen Standorten installiert sind, logisch aber wie eine Maschine behandelt werden.

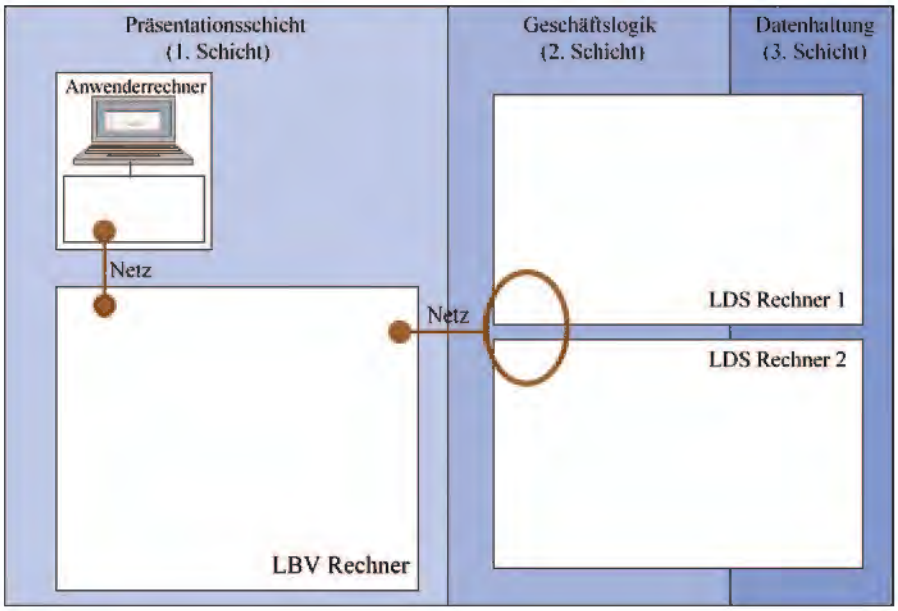


Abb. 1: Die 3-Schichten-Architektur von OBELIX

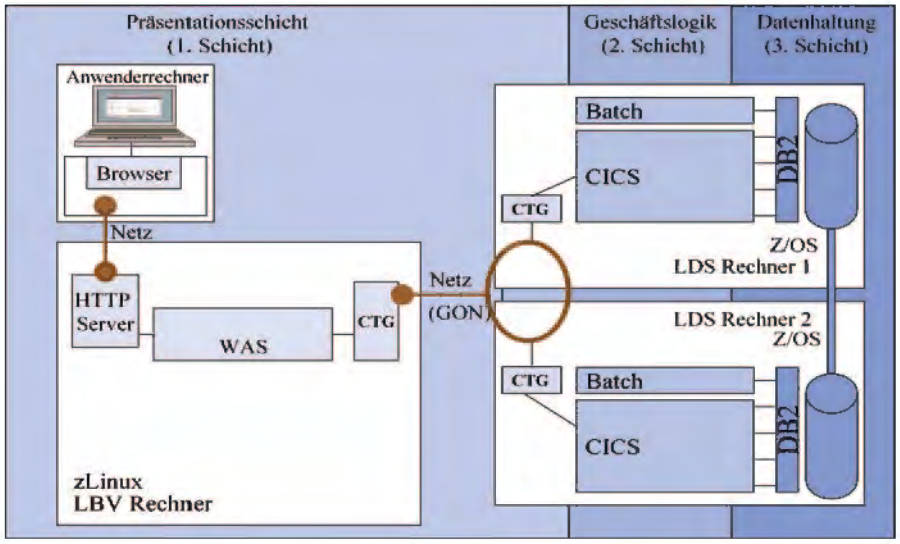


Abb. 2: Die wesentlichen technischen Komponenten von OBELIX

Architektur im LBV NRW

Zwischen dem Frontend im Browser des LBV NRW und der Geschäftslogik sowie der Datenbank auf der IBM-z900 der LDVZ wird nun eine Middleware benötigt, welche die Anfragen aus dem Browser an die Geschäftslogik vermittelt, die Ergebnisse abholt und dem Anwender wieder im Browser aufbereitet.

OBELIX ist im LBV NRW nur eines von mehreren Fachverfahren. Hier seien als weitere Fachverfahren beispielhaft nur die bausteinbasierte Textverarbeitung (eText) oder das Dokumentenmanagementsystem (DMS) erwähnt. Der Einstieg der Anwenderinnen und Anwender in die verschiedenen Fachverfahren erfolgt über eine einheitliche Benutzeroberfläche, welche die verschiedenen Anwendungen miteinander verbindet, die Anwendungsintegrations-Plattform (AIP).

Für die als Middleware eingesetzte Software wurde das Produkt „WebSphere Application Server“ (WAS) ausgewählt. Dieser Application Server wird auf dem IBM-System des LBV NRW unter zLinux betrieben und stellt u. a. die Verbindung zwischen dem Web-Browser der Anwender/-innen und den Fachverfahren über AIP her. (Abbildung 2)

Architektur im LDS NRW

Die Verbindung zwischen dem WAS im LBV NRW und den OBELIX-Programmen sowie der Datenbank auf der z900 der LDVZ erfolgt über das GON mittels des Transaktionsmonitors CICS bzw. präziser dem CICS Transaction Gateway (Details siehe unten). Die Obelix-Programme können entweder im Online-Betrieb oder im Batch-Betrieb (Stapelverarbeitung) laufen. Die Online-Programme (CICS, Details siehe unten) reagieren auf Eingaben des Nutzers. Programme im Batchbetrieb werden zur Verarbeitung großer Datenmengen genutzt, beispielsweise bei der Berechnung der Bezüge am Monatsende, wenn dies nicht schon im Online-Betrieb stattgefunden hat. Zur Datenhaltung wird eine DB2-Datenbank benutzt.

Anforderungen und Systemtechnik

Im ersten Abschnitt dieses Beitrags wurde eine Reihe wichtiger nichtfunktionaler Anforderungen aufgezählt. In diesem Abschnitt wird nun dargestellt, mit welchen Architekturentscheidungen und mit welcher Systemsoftware diese Anforderungen realisiert werden.

In Abbildung 3 ist die technische Architektur nochmals stark verfeinert abgebildet. Hier sind alle Techniken dargestellt, die helfen, die nichtfunktionalen Anforderungen an Obelix zu erfüllen. In Abbildung 4 wird darüber hinaus deutlich, wo sich die eigentlichen „OBELIX-Programme“ befinden.

Im Weiteren werden die einzelnen Techniken, die in Abbildung 3 und 4 in ihrem Zusammenspiel aufgeführt sind, im Detail vorgestellt:

Hardware und Systemsoftware

Die in der LDVZ wie auch im LBV NRW eingesetzte Hardware dient der Skalierbarkeit, und der Hochverfügbarkeit.

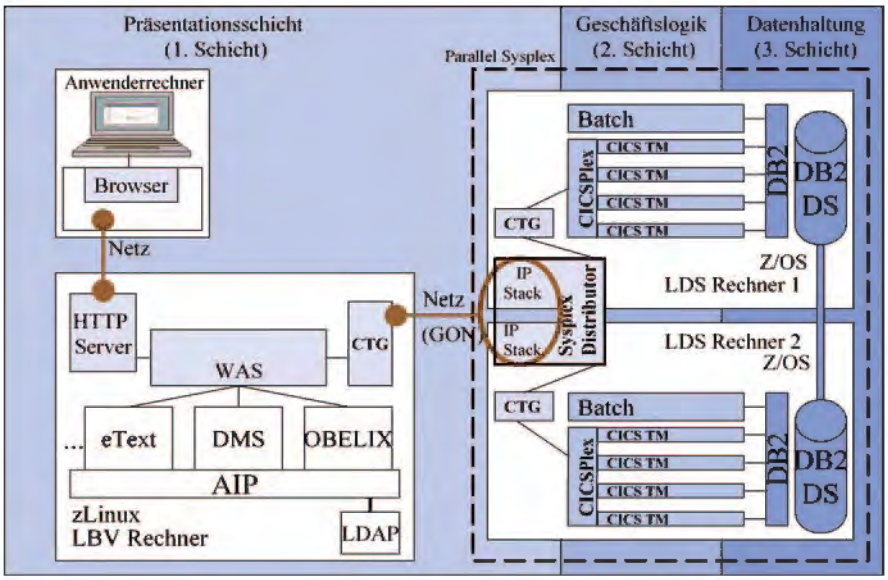


Abb. 3: Technische Architektur von OBELIX

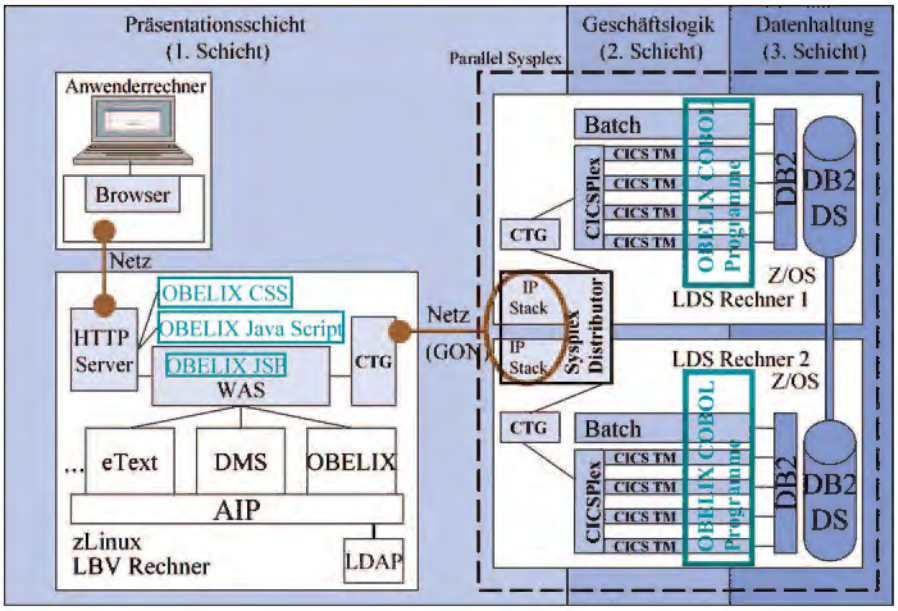


Abb. 4: Überblick über die von OBELIX verwendete Systemtechnik

Z/OS auf zSeries in der LDVZ
In der LDVZ werden Großrechner aus der IBM zSeries eingesetzt. Die Abkürzung ‚z' soll hierbei auf ‚zero down-time' hinweisen. Dies bedeutet, dass sich das System bei einem Fehler selbst wieder in einen korrekten Zustand versetzen kann (‚self-healing') und die anfallende Arbeit selbst verwalten kann (‚self-managing'), so dass die Maschine praktisch ausfallfrei laufen kann. Als Betriebssystem wird Z/OS eingesetzt.

zLinux auf zSeries im LBV
Das LBV NRW benutzt ebenfalls eine IBM-Hardware der zSeries. Auf dieser Hardware läuft das Betriebssystem Z/VM. Der WebSphere Application Server (siehe unten) benötigt als Ausführungsumgebung auf dem Z/VM eine Unix-Umgebung. Hierfür wird im LBV NRW zLinux als Arbeitssoftware unter Z/VM eingesetzt. zLinux basiert auf offenen Standards und besitzt auf der zSeries eine hohe und gute Integrationsfähigkeit für andere Softwareprodukte und Anwendungslösungen. Auf einem Rechner der zSeries kann eine große Anzahl zLinux parallel nebeneinander arbeiten. Die Rechner der zSeries sind dadurch in einfacher Form skalierbar.

Web-Technologien

Die Entwicklungsstrategie im Projekt OBELIX zielt auf ein möglichst plattformunabhängiges Frontend für den Benutzer. Hier bietet sich heute eine Web-Oberfläche basierend auf Web-Techniken an, die unabhängig von Betriebssystem und sonstiger Software mit jedem beliebigen Browser dargestellt werden kann. Die bei OBELIX eingesetzten Web-Techniken werden im Folgenden dargestellt:

Browser
Der Browser erlaubt eine grafische Darstellung, die unabhängig ist vom benutzten Betriebssystem.

Hypertext Markup Language (HTML)
HTML ist eine Sprache, die jeder Browser interpretieren kann. Die Obelix-Anwenderplattform ist dadurch unabhängig von der Technik des restlichen Verfahrens und unabhängig vom Betriebssystem des Bearbeiters.

Cascading Style Sheets (CSS)
CSS ist eine Technik, die es ermöglicht, Obelix eine ergonomische und einheitliche Oberfläche für den Anwender zu geben.

Java Script
Java Script ist eine Sprache, die für die Animation auf dem Bildschirm eingesetzt wird. Damit kann die Obelix-Oberfläche dynamisch auf Eingaben des Anwenders antworten.

Java Server Pages (JSP)
Um die obigen Techniken mit HTML zu integrieren, werden Java Server Pages eingesetzt. Diese Programmiersprache nimmt die Rohdaten aus der Geschäftslogik und bereitet eine HTML-Seite auf, die dann an den Browser auf der Anwender-Plattform geschickt wird.

WebSphere Application Server (WAS)

Für das Projekt OBELIX ist der WebSphere Application Server eine der zentralen Softwarekomponenten. Der WAS ist ein Applikationsserver, der die Funktionsaufrufe an die Geschäftslogik weitervermittelt, und die Ergebnisse an den Anwender, aufbereitet in Form von HTML-Seiten, zurückmeldet.

Die Basis des WAS wird durch eine Umgebung gebildet, die Applikationen einen umfangreichen Satz von Diensten anbietet, wie zum Beispiel Dienste, die das Transaktions-Management, die Sicherheitsanforderungen, die Performance, die Verfügbarkeit und die Skalierbarkeit der Anwendungen unterstützen. Die Steuerung und Verwaltung der WAS-Komponenten erfolgt über eine Administrations-Konsole, die die Arbeiten des Administrators u. a. bezüglich Konfiguration, Anwendungs-Verteilung und Monitoring unterstützt. Der WAS stellt außerdem die ‚Java Virtual Machine' (JVM) zur Verfügung, in der J2EE-Anwendungen (Java 2 Enterprise Edition) – im Falle von Obelix z. B. die Java Server Pages – ausgeführt werden.

Der WebSphere Application Server liefert damit eine Infrastruktur für eBusi-

ness Plattformen (siehe Abbildung 5). Der WAS ist auf vielen Plattformen einsetzbar, bei OBELIX wird er im Z/VM-Umfeld unter zLinux auf dem LBV-Großrechner eingesetzt. Im Falle einer Anbindung von Teilen des Bezügeverfahrens an das Internet käme dann ein Einsatz von WAS unter Z/OS auf der z900 der LDVZ in Betracht.

Der WAS ist zusätzlich integrierbar mit verschiedensten anderen Softwareprodukten wie:
- WebSphere Portalsoftware
- WebSphere Message Queueing
- WebSphere Business Integration
- und vielen mehr

Parallel Sysplex

Der ‚Parallel Sysplex' ist eine Anzahl einzelner Z/OS-Systeme, die über verschiedene Hardware-Komponenten und Software-Dienste zusammenarbeiten, um die anstehenden Anforderungen (Anwendungen) abzuarbeiten.

In der LDVZ besteht der Parallel Sysplex physikalisch aus zwei Maschinen, die aus Gründen der Katastrophenfallvorsorge an unterschiedlichen Standorten des LDS NRW installiert sind. Auf den zwei Maschinen vom Typ z900 werden mehrere logische virtuelle Maschinen (LPAR, Logical Partition) betrieben. Diese LPARs bilden den sog. Parallel Sysplex, d.h. alle angeschlossenen Ressourcen (Schnittstellen, Datenbanken, Programmbibliotheken) stehen jeweils allen LPARs zur Verfügung. Dies sorgt für eine besonders hohe Verfügbarkeit, da selbst bei einem Total-Ausfall einer LPAR das Verfahren auf der zweiten LPAR, die ja den Zugriff auf dieselben Ressourcen hat, weiterbetrieben werden kann. Die Leistungsfähigkeit bei einem Ausfall einer LPAR nimmt dabei natürlich ab, da nicht mehr die Prozessoren beider Maschinen zur Verfügung stehen.

Auf jeder LPAR läuft als Betriebssystem das IBM-Produkt Z/OS mit seinen Softwarekomponenten. Im Parallel Sysplex ist es möglich, die Hardware zu erweitern, ohne die Anwendungen anzufassen, d. h. die Anzahl der Prozessoren oder die Anzahl der physischen Hardwareblöcke selbst (Maschinen) zu erhöhen. Man kann die eingesetzte Sysplex-fähige Software so nutzen, dass die Hardware-Änderungen automatisch mitgenutzt werden können.

Der Parallel Sysplex ermöglicht die einfache Skalierbarkeit der eingesetzten Soft- und Hardware.

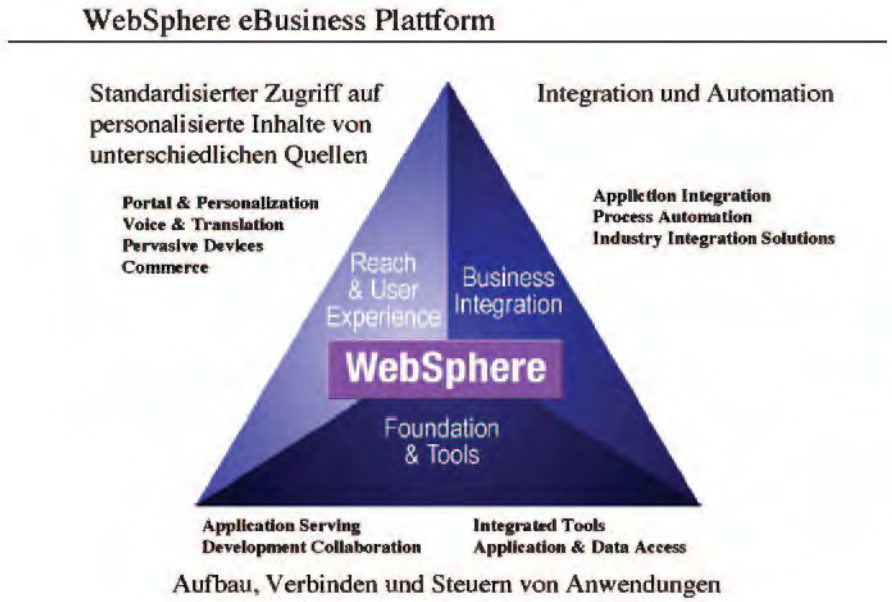


Abb. 5: IBM WebSphere eBusiness Plattform

Coupling Facility (CF)

Die Coupling Facility besteht aus eigener Hard- und Software. Sie gibt den Sysplex-fähigen Softwarekomponenten, die auf den einzelnen LPARs arbeiten, die Möglichkeit, ihre Aktivitäten zu koordinieren, indem sie Informationen in der CF ablegen oder aus der CF auslesen können. Aus Sicherheitsgründen werden mehrere CFs genutzt. Die Daten der einzelnen CFs werden untereinander gespiegelt, so dass bei Ausfall einer CF eine andere deren Arbeit mit übernehmen kann. Damit wird die Anforderung der Hochverfügbarkeit gestützt.

Workloadmanager (WLM)

Der Workloadmanager ist eine Softwarekomponente des Z/OS mit erweiterter Funktionalität im Parallel Sysplex. Diese erweiterte Funktionalität dient dazu, einzelne Ressourcen – wie z. B. CICS, LPAR – übergreifend anzusteuern.

In dem er die Nutzung der auf beiden LPARs verfügbaren Ressourcen überwacht und gleichzeitig durch Lastverteilung eine gute Performance der aktiven Ressourcen ermöglicht, gewährleistet der WLM die Hochverfügbarkeit der OBELIX-Anwendung. Er unterstützt außerdem eine gute Perfomance von Obelix. Im Rahmen der Entwicklung der Obelix-Anwendungen wird darauf geachtet, dass die Arbeit des WLM unterstützt und für Obelix genutzt wird.

Sysplex Distributor (SD)

Das Konzept der virtuellen Portadressen für TCP/IP ist die Basis für die Arbeiten des Sysplex Distributors (SD). Er übernimmt innerhalb der TCP/IP-Umgebungsverwaltung auf Z/OS eine Funktion, die es erlaubt, eine vir-

tuelle IP-Adresse dynamisch auf die LPARs gleichzeitig zu verteilen (TCP Port Sharing). Der SD sorgt ferner für eine Lastverteilung unter Einbeziehung des WLM und nutzt in der CF stehende Informationen für seine Arbeiten.

Das LDS NRW setzt im Projekt OBELIX den Sysplex-Distributor ein, um die Anforderungen an Hochverfügbarkeit der Anwendungen und an eine gute Performance zu erfüllen.

CICS Transaction Server (CICS TS)

Ein CICS Transaction Server (im Weiteren auch kurz CICS) hat die Aufgabe die Transaktionen zu koordinieren. Es führt die Anwendungen aus, koordiniert alle durch die Anwendung benötigten Ressourcen, wie die Zugriffe auf DB2 (siehe unten) sowie das Benutzen von Dateisystemen und stellt verschiedene Dienste zur Verfügung. Außerdem sorgt es dafür, dass alle in den CICS-Anwendungen benutzten Ressourcen/Daten, z. B. die Daten im DB2, integer gehalten werden.

Bei einer Transaktion gilt, dass Veränderungen zwischen zwei gewählten Synchronisationspunkten überall oder gar nicht durchgeführt werden. Um diese Aktivitäten, die Daten integer zu halten, braucht sich der Anwendungsentwickler nicht zu kümmern, sie erfolgen über CICS automatisch. Automatische Restart- und Recovery-Mechanismen erlauben eine sichere Handhabung des CICS.

CICS unterstützt die Performance dadurch, dass Programme möglichst selten geladen werden, sondern statt dessen sofort aus dem Arbeitsspeicher heraus ausgeführt werden und damit sehr schnell arbeitsfähig sind. Sicherheitseinrichtungen sorgen zusätzlich dafür, dass sich die einzelnen Programme ihre Speicherbereiche nicht unbemerkt überschreiben können.

Die Aktivitäten der einzelnen Transaktionen können durch Monitoring (CICS PM) und durch das Führen von Statistiken für den Nutzer sichtbar gemacht werden.

In der LDVZ wird CICS schon viele Jahre genutzt und das Projekt OBELIX kann auf vorhandenes Wissen und Erfahrungen zurückgreifen.

CICSPlex System Manager (CICSPlex SM)

Der CICSPlex System Manager (CICSPlex SM) ist ein System Management Tool, das es ermöglicht, einen Verband von mehreren CICS so darzustellen, als wäre es nur ein einzelnes CICS. Die Verteilung der Arbeitslast auf die verschiedenen CICS übernimmt dann der CICSplex SM. Der CICSPlex SM ist Bestandteil der CICS Familie.

Die Verwaltung der in einem CICSplex arbeitenden Einzel-CICSe wird durch zentralisierte Funktionen so erleichtert, dass von einer Stelle aus alle Ressourcen verwaltet werden können („single point of control“).

Der CICSplex SM arbeitet bezüglich der Verteilung der durchzuführenden Anwendungen auf die einzelnen CICSe eng mit dem WLM zusammen. Verteilung der durchzuführenden Anwendungen bedeutet, dass auch CICSe, die auf anderen LPARs liegen, miteinbezogen werden. Der CICSPlex SM erhöht dadurch die Performance von Obelix.

CICS Transaction Gateway (CTG)

Das CICS Transaction Gateway dient als CICS-Connector. Es liefert die Möglichkeit, Web-Anwendungen, so genannte Client-Applikationen, die auf verschiedenen Hardware- und Software-Plattformen laufen, mit dem CICS zu verbinden. Hierbei werden Standard-Internet-Protokolle verwendet. Die Kommunikation zwischen den Client Anwendungen und dem CTG kann die folgenden Protokolle nutzen:

- TCP/IP (Transmission Control Protocol /Internet Protocol)
- http (Hypertext Transfer Protocol)
- SSL (Secure Socket Layer)
- HTTPS (http über SSL)

Eingesetzt wird das CTG im Projekt OBELIX, um die physisch verteilte Präsentationslogik (Java-Programme unter WAS) und die Geschäftslogik (COBOL-Programme unter CICS) miteinander zu verbinden.

Das Java-Programm auf dem LBV-Rechner nutzt die CTG-Java-Klassen, um über den CTG-Daemon auf dem Host die Programme im Host-CICS aufzurufen (siehe Abbildung 6).

COBOL II

COBOL II ist eine 3GL-Sprache, die auf vielen Plattformen vorhanden ist. Sie wird auf dem LDS-Rechner unter Z/OS für die Durchführung der Ge-

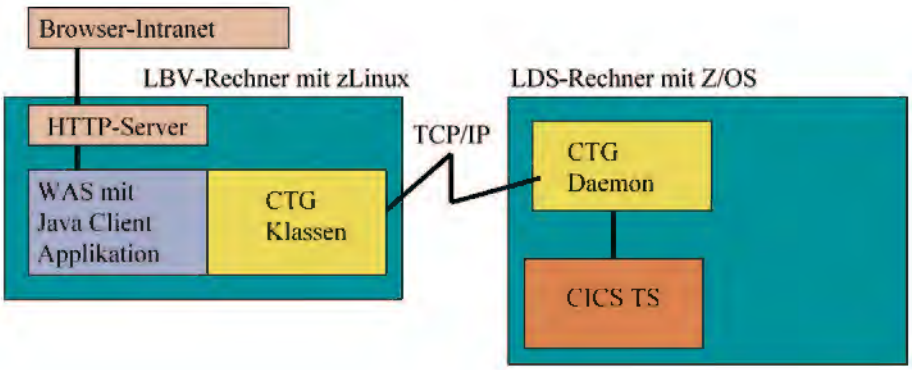


Abb. 6: Zugriff der Präsentationsschicht (LBV NRW) über CTG auf die Geschäftslogik (LDS NRW)

schäftslogik benutzt sowohl für die Web-Transaktionen (Online-Zugriffe von Nutzern) als auch für die Batch-Programme (Stapelverarbeitung). Der COBOL II-Code ist das Ergebnis der Generierung aus dem im Projekt OBELIX eingesetzten Entwicklungstool Visual Age Generator, einem 4GL-Tool.

Gemäß den Erfahrungen der LDVZ ist COBOL II eine sehr performante Ausführungssprache. Zusätzlich sind Erfahrung und Wissen für den Umgang mit COBOL II vorhanden.

DB2

Das DB2 ist eine Datenbanksoftware von IBM für die Bearbeitung relationaler Daten, die auf vielen Plattformen arbeiten kann. Für das Projekt OBELIX wird DB2 im Z/OS-Umfeld verwendet.

DB2 ist ein hochperformantes und hochverfügbares Datenbanksystem, das die Umsetzung der nichtfunktionalen Anforderungen unterstützt. Ein eigenes Sicherheitssystem, das in enger Zusammenarbeit mit RACF (Ressource Access Control Facility) bei Nutzung des Z/OS Betriebssystems steht, schützt gegen unerlaubten Zugriff (Datensicherheit).

DB2 erlaubt in der verfügbaren Version nahezu einen „Rund um die Uhr"-Betrieb. Mit Hilfe der Sprache SQL (Structured Query Language) werden dem DB2 die Aufforderungen zur Bearbeitung der Daten übergeben. Mit seinen Such- und Sperr-Mechanismen bearbeitet es die angeforderten Anfragen performant und sicher. Es ist hierbei in der Lage, die vorhandene Prozessorleistung und den verfügbaren Arbeitsspeicher effizient zu nutzen. Monitorsysteme erlauben eine permanente Überwachung der laufenden Arbeiten, OBELIX setzt zur Überwachung von DB2 den DB2 Performance-Monitor ein.

DB2 Data Sharing (DB2 DS)

Im Projekt OBELIX wird das DB2 Data Sharing benutzt. Beim DB2 Data Sharing werden die DB2-Datenbanken, die auf den beiden z900-Maschinen laufen, miteinander verbunden. Mit DB2 Data Sharing ist es möglich, auf jedem der beteiligten physischen z900-Server die zu bearbeitenden Daten der gleichen Datasets konkurrierend zu bearbeiten. Die Server haben die Daten in ihren eigenen Arbeitsspeichern zur Verfügung. Datenkonsistenz wird über die CF mit ihrem Speicher und den Global-Lock-Mechanismen, die durch den Betriebssystemseitigen Lock Manager verwaltet werden, sichergestellt.

Data Sharing:

- erhöht die Verfügbarkeit der Daten. In unserem Falle können die DB2-Datenbanken auf den beiden LPARs physisch unabhängig die gleichen Datasets bearbeiten. Wenn eine Maschine ausfällt, kann die andere noch arbeiten. Im Rahmen des Data Sharing wird die CF genutzt, um Informationen der einzelnen DB2-Member verfügbar zu halten.
- wird im Projekt OBELIX dazu genutzt, große Datenmengen bis zu 10fach parallel mit dem gleichen Batch-Programm abzuarbeiten. Technisch wird dieser Vorgang unterstützt, indem die Daten der DB2-Tabellen im Rahmen des technischen Designs entsprechend partitioniert werden.
- wird durch den WLM gestützt und ermöglicht damit die softwareseitige Steuerung der Performance.

In der LDVZ wird DB2 schon viele Jahre eingesetzt, so dass das Projekt OBELIX auf vorhandenes Wissen und Erfahrungen zurückgreifen kann.

In folgender Tabelle werden nochmals die einzelnen, oben beschriebenen technischen Komponenten von OBELIX mit ihrer Bedeutung für die Verwirklichung der nicht-funktionalen Anforderungen dargestellt. Insgesamt dient die eingesetzte Technik dazu, die an OBELIX gestellten hohen Anforderungen zu erfüllen.

Zusammenhang zwischen verwendeten Systemkomponenten (Zeilen) und nichtfunktionalen Anforderungen (Spalten) bei OBELIX

	Plattform-unabhängiges Frontend	Performance	Datensicherheit und Katastrophenschutz	Datenschutz und Revisionssicherheit	Skalierbarkeit	Hochverfügbarkeit
Web-Technologie	x					
WebSphere Application Server	(x)	x				(x)
z900 Hardware		x	x		x	x
Parallel Sysplex		x	x		x	x
Coupling Facility		x	x		x	x
Workloadmanager		x				x
Sysplex Distributor		x	x		x	x
RACF				x		
COBOL II		x				
CICS TS		x	x			
CICSPlex		x			x	x
DB2		x	x	x		
DB2 Data Sharing		x	x		x	x

Fazit und Ausblick

In diesem Artikel wurde die Architektur von OBELIX und die derzeit eingesetzte Systemtechnik dargestellt. Dabei wurde insbesondere auf den Zusammenhang zwischen der Systemsoftware und der zugrunde liegenden Kundenanforderung eingegangen.

In der nächsten Realisierungsstufe wird der Bereich der Angestelltenvergütung Mitte 2005 in Produktion genommen. Dieser Stufe folgt dann die Übernahme der Pensionärsversorgung nach OBELIX. Als Termin hierfür ist Ende 2005 geplant. Diese beiden wichtigen Meilensteine lassen sich mit der gegenwärtig entwickelten Systemarchitektur und Systemtechnik umsetzen.

In einem weiteren Schritt, der bislang zeitlich noch nicht festgelegt ist, beabsichtigt das LBV NRW Teile von OBELIX dem Bezügeempfänger direkt über das Internet zugänglich zu machen. Hierfür sind Veränderungen in der Systemtechnik erforderlich, wie z. B. ein Zugang der User über das „unsichere“ Internet. Für die ersten Releasestufen ist der Zugang der Bearbeiter/-innen nur über das „sichere“ Landesverwaltungsnetz erforderlich. Somit sind zur Zeit deutlich niedrigere Anforderungen an IT-Security zu stellen, als dies dann bei der Öffnung über das Internet erforderlich sein wird.

Wenn Obelix über das Internet zugänglich ist, ist eine Veränderung der bisherigen technischen Architektur nötig. Der Internet-Zugang wird über das LDS NRW erfolgen, d. h. über den LDS-Großrechner. Im Einzelnen bedeutet dies, dass auf dem LDS-Großrechner eine AIP-Komponente vorhanden sein muss, die die Präsentationsebene umfasst und die Rechteüberprüfung übernimmt. Darüber hinaus müssen dann alle drei Schichten auf einem Rechner, dem LDS-Großrechner liegen.

Auch muss der Zugang aus dem Internet über eine so genannte demilitarisierte Zone (DMZ) erfolgen, ein System aus hintereinandergeschalteten Firewalls, um eine höchstmögliche Sicherheit vor unberechtigten Zugriffen aus dem Internet zu bieten.

Guido Winkler
Telefon: 0211 9449-5371
E-Mail: guido.winkler@lds.nrw.de

Eberhard Baumgarten (IBM)
Telefon: 0211 9449-5439
E-Mail: ebaumga1@de.ibm.com

Abkürzungen/Glossar

3GL	Sprache der dritten Generation
4GL	Sprache der vierten Generation
AIP	Anwendungs-Integrations-Plattform. Einstieg der LBV-Bearbeiter in die Fachverfahren des LBV
Batch	Stapelverarbeitung
CCS	Cascading Style Sheets
CICS	Customer Information Control System, Transaktionsmonitor
CICSPlex SM	CICSPlex System Manager
CICS PM	CICS Performance Monitor
CICS TS	CICS Transaction Server (synonym CICS)
CF	Coupling Facility
CTG	CICS Transaction Gateway
DB2	DB2 Universal Database für OS/390 und Z/OS
DB2-DS	DB2 Data Sharing
DB2 PM	DB2 Performance Monitor
DMS	Dokumentenmanagementsystem
DMZ	Demilitarisierte Zone
eText	Bausteinbasiertes Textverarbeitungssystem des LBV
GON	Glasfaser Overlay Netz
HTML	Hypertext Markup Language
http	Hypertext Transfer Protocol
https	http über SSL
J2EE	Java 2 Enterprise Edition
JSP	Java Server Pages
LDAP	Lightweight Directory Access Protocol
LPAR	Logical Partition, logische Maschine auf der IBM z900
OBELIX	Online-Bezügeverfahren des Landes NRW mit internen und externen Ressourcen
RACF	Ressource Access Control Facility
SD	Sysplex Distributor
SQL	Structured Query Language
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol /Internet Protocol
WAS	WebSphere Application Server, IBM-Middleware für die Verbindung zwischen dem Frontend im Browser und der Geschäftslogik und Datenbank
WLM	Workloadmanager
z900	derzeit von der LDVZ eingesetzter IBM-Großrechner der Serie z900
z/Linux	Linux-Variante für die IBM zSeries
Z/OS	Betriebssystem auf der z900


Index 2000 – 2004

Ausgabe	Schwerpunktthema
1/2004	SPAM – und (k)ein Ende?
	Open Source Software auf Webservern im LDS NRW
	Gefahren durch Viren
	OBELIX und die Systemtechnik
2/2003	SAPOS® – ein modernes Werkzeug zur Positionsbestimmung und Vermessung – realisiert durch Kooperation der Landesbetriebe
	SPAM – Wenn der Postmann zwei(tausend)mal klingelt
	Zentrale Problemkoordinierung durch das IT-Managementzentrum
	ArcGIS-Entwicklungen des Graphikzentrums im LDS NRW – Automatisch erzeugte Kartenrahmen für ArcGIS 8.x –
	Internetzugang der Landesverwaltung NRW
	Landesdatenbank im Web – Status und Planung
	Datendrehscheibe – Einleiterüberwachung – Abwasser D-E-A: Stand und Entwicklungsperspektiven
	DV-technisches Systemdesign im Projekt Obelix
	Wie hältst Du's mit den EJBs? Webanwendungen mit Java im Überblick
1/2003	GeoServer der Landesverwaltung NRW nimmt Produktion auf
	Angebot zentraler GIS-Dienste mit dem GeoServer
	Landtagsinformationssystem NRW
	Microsofts .Net-Technologie – wohin geht die Programmierung?
	Programmierung mit dem VisualAge Generator im Projekt OBELIX
	Webhosting-Dienstleistungen des LDS NRW

Ausgabe	Schwerpunktthema
1/2002	**Einführung des Geoinformationssystems „ArcGIS“ in der Landesverwaltung NRW mit Unterstützung des Grafikzentrums im LDS NRW**
	Testmanagement und Testautomatisierung im Projekt Obelix
	Contentmanagement in NRW **Ausbau der Webinformationsangebote der Landesverwaltung und Erleichterung des Zugangs zu Informationen**
	FÜSYS **Ein Führungsinformationssystem zum strategieorientierten Management erfolgsrelevanter Projekte in Ministerien und anderen großen Behörden**
	SAN macht Daten schnell **Storage Area Network im Windows-LAN des LDS NRW**
	Die Netzbasis des Landesverwaltungsnetzes – gerüstet für die Zukunft
	'Penguin meets Dinosaur' **Linux und Großrechner finden zueinander**
2/2001	
	Das Internet als neues Medium für die Erhebung statistischer Daten
	Dienstleistungen und Servicekonzepte des LDS NRW zur IT-Infrastruktur
	Die Erhebung der Abwasser abgabe – DV-Unterstützung einer gesetzlichen Aufgabe
	GEOSERVER der Landesverwaltung NRW im Intranet und Internet
	Der Umweltdatenkatalog NRW **Transparente Umweltinformationen für Öffentlichkeit, Politik und Planung**
	Kostensenkung am PC-Arbeitsplatz durch Geschäftsprozessanalyse im Desktop Management des LDS NRW
	Bibliotheksverbund der Landesbehörden NRW
	Web Based Training im Landesverwaltungsnetz

Ausgabe	Schwerpunktthema
1/2001	**Kommunikation ist alles – Elektronische Post**
	Landtagsinformationssystem Nordrhein-Westfalen
	Public Key Infrastruktur – Was steckt dahinter?
	Normen zur Software-Ergonomie
	IT-Unterstützung im Support – Nutzung eines Trouble-Ticket-Systems
	„Gut Werkzeug – halbe Arbeit“ Unterstützung der Anwendungsbereitstellung durch Vorgehensmodelle, Methoden und Werkzeuge
	Obelix – das neue Bezügeverfahren
2/2000	**LDS NRW – Internet-Dienstleister der Landesverwaltung Nordrhein-Westfalen**
	Web-Anwendungen auf dem IBM-Großrechner
	Lehrereinstellungsverfahren in Nordrhein-Westfalen
	Spracherkennungssoftware – schon einsatzbereit?
	Integriertes Netz- und Systemmanagement – Selbstzweck oder Wunderwaffe?
1/2000	**Das Büro auf Reisen Mobilität und Datenaktualität – mobile computing Mobile Telefone, Smartphones, Handhelds, PDAs, Notebooks – eine Bestandsaufnahme**
	IT-gestützte Vorgangsbearbeitung in der Landesverwaltung Nordrhein-Westfalen
	DV-Vorhaben D-E-A (Datendrehscheibe, Einleiterüberwachung, Abwasser)
	Zertifizierung des IT-Qualitätsmanagements der LDVZ nach DIN EN ISO 9001
	Das Windows-NT-Netz im LDS NRW