Baden-**W**ü**r**ttembergs **e**xtended **l**an

BelWü

BelWü-Koordination

BelWü / LVN Sicherheitskonzept

Anbindung der BelWü-Teilnehmer
über das BelWü-Backbone an
das Landesverwaltungsnetz
mittels Web-Proxy und VPN
V 1.0 vom 10.07.2003

Inhaltsverzeichnis

Kapitel 1

Einleitung

Der Zweck dieses Papiers ist die Darstellung eines sicheren und kostengünstigen Zugangs von BelWü-Teilnehmern zu ausgewählten LVN-Diensten. Dies erfolgt über vom normalen Arbeitsplatz mittels VPN zu einem Web-Proxy.

BelWü steht für "Baden-Württembergs extended LAN" und ist das Datennetz der wissenschaftlichen Einrichtungen und Schulen des Landes Baden-Württemberg. Es verbindet zur Zeit ca. 240 000 Computer von ca. 2600 Teilnehmern (Stand: Mai 2003) miteinander. Das besondere in diesem Umfeld sind zwei Aspekte:

1. Es werden Hochgeschwindigkeitsverbindungen mit n * 2,4 Gbit/s zwischen den Universitäten des Landes genutzt (siehe hierzu http://www.belwue.de/info/gbit/BelWue-Topologie-Lambda.gif).
2. Das BelWü ist das einzige Regionalnetz der Bundesrepublik in der Wissenschaftswelt, das zentral verwaltet wird.

BelWü versteht sich als ein Zusammenschluß der baden-württembergischen Hochschulen und Forschungseinrichtungen zur Förderung der nationalen und internationalen Telekooperation und Nutzung entfernt stehender DV-Einrichtungen unter Verwendung schneller Datenkommunikationseinrichtungen. Unbeschadet der innerorganisatorischen Eigenständigkeit der Hochschulrechenzentren ist das Kernziel die Darstellung dieser Rechenzentren als eine einheitliche DV-Versorgungseinheit gegenüber den wissenschaftlichen Nutzern und Einrichtungen.

An jeder Hochschule steht ein zentraler Router, der den Verkehr zwischen BelWü-Netz und Hochschule regelt. Dieser wird vom zentralen Netzwerkmanagement des BelWü betreut. Die Router befinden sich in einem gesicherten Raum des Rechenzentrums der jeweiligen Hochschule. Der Zugang auf den Router ist mit Access-Listen und Passwörtern geschützt. Zugriffsberechtigung hat das IP-Management der BelWü-Koordination.

Das BelWü/LVN Sicherheitskonzept wird stufenweise aufgebaut. In der ersten Stufe wird der Zugang mittels LVN-Einzelplatz-PC beschrieben; in einer folgenden Stufe wird der Zugang mittels LAN behandelt. In der hier vorliegenden dritten Stufe wird der Zugang über einen normalen Arbeitsplatz mittels VPN zu einem Web-Proxy und dann zu ausgewählten LVN-Anwendungen beschrieben. Im vorliegenden Papier werden sicherheitsunkritische Anwendungen wie LVN-ID, Vorschriftendienst, Fortbildung 21, NSI-Informationen, MSWEB und Büroshop des LZP erläutert. Bei einem weiteren Bedarf von zusätzlichen Anwendungen oder veränderten Betriebsbedingungen wird das Konzept fortgeschrieben. Weitere Anwendungen könnten Angebote des LBV, MLR, UVM und StaLa umfassen.

Kapitel 2

Wirtschaftlichkeitsberechnung

Die Kosten der Zugangs über den normalen Arbeitsplatz, VPN und Web-Proxy ist im Vergleich zur konventionellen LVN-Einzelplatz-PC Anbindung wesentlich geringer:

Bei der angestrebten Web-Proxy Lösung treten keine zusätzlichen Kosten für PC und Verschlüsselungsbox beim Nutzer auf. Die VPN Clientensoftware (von Cisco) ist kostenfrei verfügbar. Auf Seiten der BelWü-Koordination treten Hardwarekosten für einen Cisco VPN3015 Concentrator zu ca. 10.000 Euro auf. Für den Web-Proxy kann einen vorhandene SUN verwendet werden.

Bei der konventionellen LVN-Einzelplatz-PC Anbindung treten pro Zugang Hardwarekosten (Cisco1605 mit je 1250.- Euro) auf. Bei ca. 100 Zugängen wären die einmaligen Gesamtkosten 125.000 Euro.

Von Seiten des ZKD wird nach derzeitigem Stand der Aufwand beim ZKD für die Web-Proxy Lösung als geringer betrachtet.

Kapitel 3

Sicherheitskonzept

3.1 IT-Sicherheitshandbuch

Die folgende Risikobewertung orientiert sich an den Handbüchern des BSI (IT-Grundschutzhandbuch, IT-Sicherheitshandbuch).

3.1.1 IST-Aufnahme

Derzeit erfolgt die Kommunikation zwischen BelWü-Teilnehmern und dem LVN über folgende Kanäle:

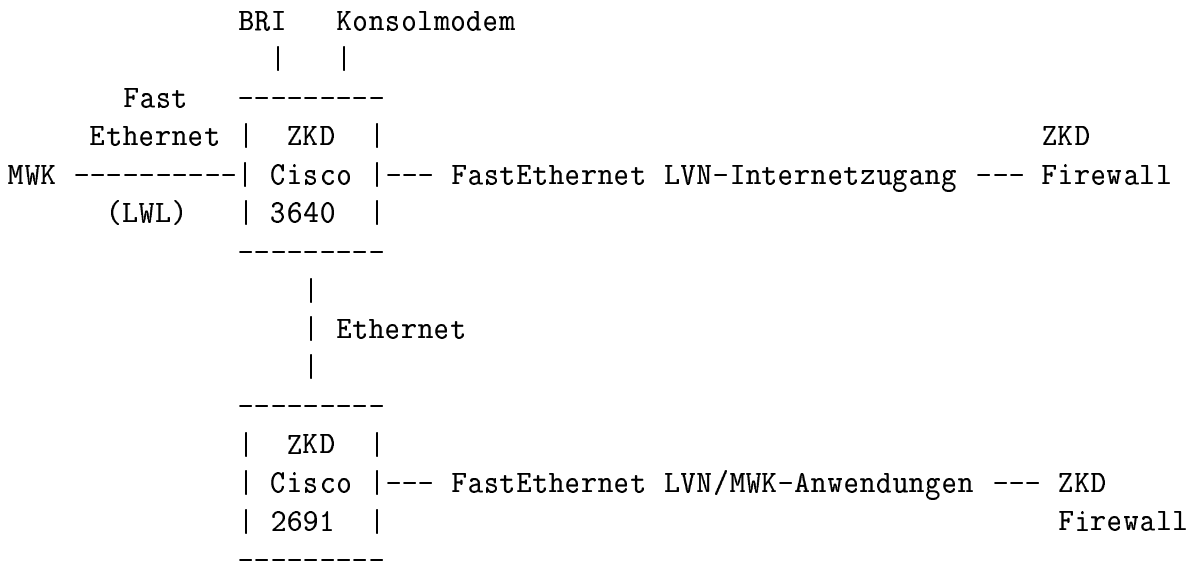
- Mailaustausch über das öffentliche Internet (per SMTP).
- Zugang zu LVN-Anwendungen wie NSI über einen IPSec Tunnel zwischen LVN und Einzelplatz-PC über BelWü.
- Zugang zu LVN-Anwendungen wie NSI über einen IPSec Tunnel zwischen LVN und LAN einer BelWü-Hochschule.

Vor der LVN Phase III gab es folgende Zugangsmöglichkeiten:

- Zugang zum StaLA (LIS) über ein telnet/3270 SNA Gateway zwischen BelWü und LVN.
- Direkter Zugang zum LVN über einen direkten LVN Phase II Zugang.

Durch die Migration des LVN zur Phase III fielen die letzten beiden Kommunikationsmöglichkeiten weg. Sie wurden durch die per IPSec verschlüsselte Kommunikation über die BelWü-Infrastruktur ersetzt. Die technische Realisierung ist wie folgt:

Als Netzwerkprotokoll wird nur TCP/IP zugelassen. Das Landesverwaltungsnetz ist derzeit mit einer 100 MBit/s FastEthernet-Leitung über Lichtwellenleiter (LWL) an den BelWü-Backbone angebunden und endet auf einem Cisco-Router am Wissenschaftsministerium (MWK). Das andere Ende der Leitung bildet ein Cisco3640 am ZKD, der ebenfalls von der BelWü-Koordination betreut wird.

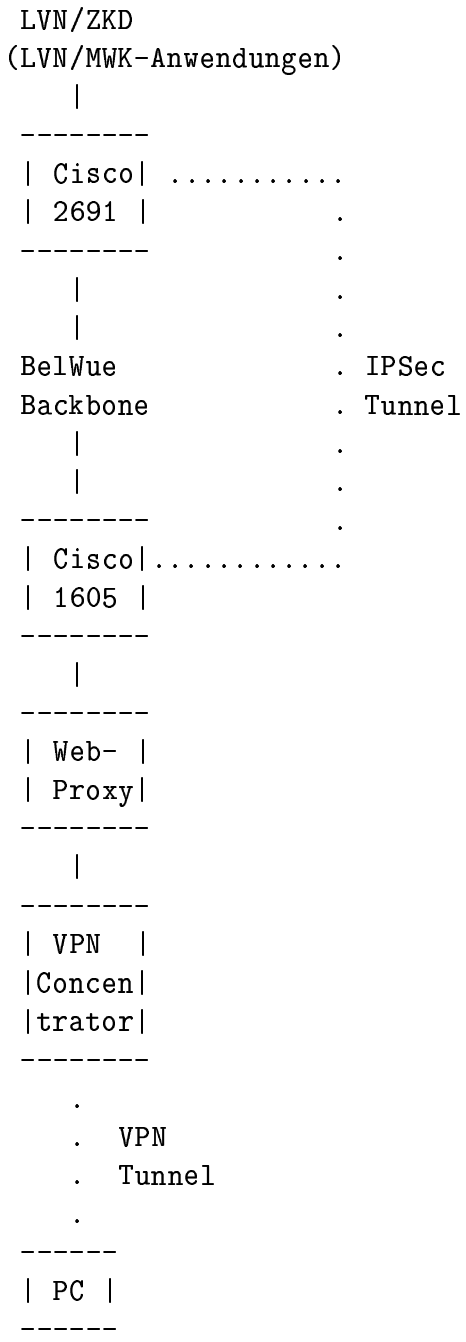


Um die Zuständigkeiten zwischen BelWü und LVN besser abzugrenzen, wurde in Absprache mit dem ZKD der Cisco3640 mit drei Ethernetinterfaces beim ZKD installiert. Dadurch ergeben sich zwei Ethernetinterfaces zum ZKD - eins für den (öffentlichen) Internetzugang des LVN und das andere für die LVN/MWK-Anwendungen (wie DIPSY, NSI, etc.). Zusätzlich sorgt ein mehrfach passwortgeschützter Modemzugang auf die Routerkonsole (für Notfallwartungen) sowie ein BRI-Interface mit ISDN (letzteres als Backup falls die 100 MBit/s Leitung ausfällt) für mehr Betriebssicherheit.

Im April 2003 wurde für die LVN/MWK-Anwendungen (wie DIPSY, NSI, etc.) ein eigener Router (Cisco2691 mit Hardwareverschlüsselungsmodul) eingesetzt. Auf diesem Router (ZKD-2691) enden alle IP-Tunnel der angeschlossenen BelWü-Teilnehmer. Um eine ausreichende Sicherheit zu erreichen, werden die Tunnel mit IPSec (DES und 3DES) verschlüsselt.

Durch Access-Listen wird der IP-Verkehr so gesteuert, dass Zugriffe vom öffentlichen Internet nicht möglich sind. Außerdem wird durch Accesslisten die Kommunikation auf PC und LVN-Server begrenzt, genauer gesagt, auf die notwendige Anwendung (Port). IP-Spoofing wird auf Tunnelseite des ZKD-2691 durch Access-Listen unterbunden. Der Zugriff der verschiedenen angeschlossenen Einrichtungen untereinander wird durch geeignete Access-Listen auf die Tunnel-Interface unterbunden.

3.1.1.1 Anbindung über VPN und Web-Proxy



Der VPN-Tunnel wird hier von einem Arbeitsplatz-PC mittels der Cisco VPN Clientsoftware zu dem VPN Concentrator aufgebaut. Hierüber wird per http (TCP Port 80) der Web-Proxy angesprochen.

Der Web-Proxy ist mittels eines Apache Servers auf einer SUN Workstation mit Betriebsystem Solaris, Release 8 realisiert. Auf dieser SUN läuft der Apache Server

als alleiniger Dienst.

Der Web-Proxy erreicht ausgewählte LVN Anwendungen über einen IPSec-Tunnel zwischen dem Cisco2691 beim ZKD und einem dedizierten Cisco1605. Anstelle des Cisco1605 kann auch ein kostengünstigerer und leistungsfähiger (3DES in Hardware) Cisco831 verwendet werden. In diesem Konzept kann daher "Cisco1605" an allen Stellen (außer 3DES) durch "Cisco831" ersetzt werden. Der Web-Proxy (lvn-proxy.belwue.de) verwendet als IP-Adressen 10.15.48.10 (privat) und 129.143.4.82 (öffentlich).

Vorteil des Konzeptes ist, dass es zu keinen Inkompatibilitäten zwischen VPN Clientsoftware und VPN Concentrator kommt. Der VPN Concentrator wird von der BelWü-Koordination konfiguriert und betreut; ebenso der Web-Proxy und die IPSec Verbindung zum ZKD. Dadurch können auch einzelne Teilnehmer einer BelWü-Hochschule ohne Extrakosten auf Seiten des Teilnehmers an das LVN mit ausreichender Sicherheit angebunden werden, da keine zusätzliche Hardware beim Teilnehmer notwendig ist.

Nachteil dieses Systems ist die Beschränkung des Zugangs auf nur wenige unkritische, ausgewählte Anwendungen beim LVN. Dies sind momentan:

- LVN-ID:
  www.lvn-id.bwl.de (10.127.255.100).
- Vorschriftendienst Baden-Württemberg:
  www.vd-bw2.bwl.de (10.127.255.35, 10.127.255.36).
- Fortbildung 21:
  www.fobi21.bwl.de (10.127.255.111).
- NSI:
  - NSI-Portal:
  www.nsi.bwl.de (10.125.248.17).
  - NSI-Online-Server:
  www.nsi-online.bwl.de (10.127.255.112).
  - NSI-E-Learning:
  www.on-demand.bwl.de (10.125.237.12).
- MSWEB:
  (10.127.255.140).
- Büromittel-Shop des Logistikzentrums der Polizei:
  www.lzp.bwl.de (10.127.255.62).
  Dieser ist inzwischen auch über das öffentliche Internet unter www.shop.lzp.de erreichbar.

- DNS-Server:
  10.127.255.130, 10.127.255.131.

3.1.2 Risikobewertung

3.1.2.1 Bedrohungsanalyse

Hinsichtlich der Bedrohung muss unterschieden werden, ob der Arbeitsplatz-PC beim BelWü-Teilnehmer oder der Server beim LVN betroffen ist. Bedrohungen sind Verlust der Verfügbarkeit, Integrität und der Vertraulichkeit der IT-Anwendungen und Informationen. Dazu gehören z.B. unberechtigtes Lesen, Verändern oder Löschen der Daten.

Die Bedrohung ergibt sich primär dadurch, dass Daten unverschlüsselt über Netzinfrastrukturen gehen, die nicht direkt der Kontrolle der teilnehmenden Einrichtung untersteht.

Andere Bedrohungen wie z.B. aufgrund höherer Gewalt oder technisches Versagen werden in diesem Papier nicht behandelt.

3.1.2.2 Ermittlung des Schutzbedarfs

Als Schutzziele werden definiert der Schutz der sicherheitsrelevanten Daten und Anwendungen vor Bedrohungen von außen sowie die Sicherung der Verbindung zwischen BelWü-Teilnehmer und LVN.

Der Schutzbedarf hängt von den Anwendungen ab. Ein hoher Schutzbedarf wird für EPVS und NSI angenommen; für LIS ein geringer bis mittlerer Schutzbedarf; für die Literaturdatenbank beim StaLA, LVN-ID, Vorschriftendienst, Fortbildung 21, NSI-Informationen, MSWEB sowie Büroshop des LZP ein geringer bis gar keiner.

3.1.2.3 Risikoanalyse

Das Risiko eines Angriffes aus dem LVN auf den PC des BelWü-Teilnehmer kann als sehr gering angesehen werden, da aufgrund von Router-Accesslisten eine Kommunikation nur zwischen PC und definierten LVN-Endsystemen (Servern) möglich ist. Diese Server werden als "sicher" betrachtet, da sie gut gepflegte Systeme darstellen.
Maßnahmen: Nummer 16
Risikobewertung hinsichtlich des Auftretens: sehr gering.
Risikobewertung hinsichtlich des Schadens: sehr gering.

Das Risiko eines Angriffes über den PC des BelWü-Teilnehmer auf den LVN-Server wird als gering angesehen, da der PC u.a. durch die eingebaute Firewallsoftware des

Cisco-VPN-Client geschützt wird und die Kommunikation zwischen PC und Server mittels IPSec verschlüsselt wird.
Maßnahmen: Nummer 1 bis 12, 16
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: gering.

Ein weiteres Risiko besteht darin, dass unbefugte Personen durch Konfigurationsänderungen des VPN Concentrators, Web-Proxy bzw. Cisco2691 Zugriff auf die übermittelten Daten erhalten bzw. Zugang zum LVN erhalten. Die Auswirkungen können durch zusätzliche Accesslisten auf dem LVN-Firewall minimiert werden.
Maßnahmen: Nummer 17
Risikobewertung hinsichtlich des Auftretens: sehr gering.
Risikobewertung hinsichtlich des Schadens: mittel.

Ein weiteres Risiko besteht darin, dass unbefugte Personen durch elektromagnetisches Abhören des PC-Bildschirmes Informationen über die Datenkommunikation erhalten. Da dieser Aufwand recht hoch ist und dadurch keine Daten verändert werden können, wird dieses Risiko als tolerabel hingenommen.
Maßnahmen: keine
Risikobewertung hinsichtlich des Auftretens: sehr gering.
Risikobewertung hinsichtlich des Schadens: sehr gering.

Ein weiteres Risko besteht darin, dass unbefugte Personen den Datenverkehr innerhalb des BelWü, innerhalb des LVN bzw. auf dem LVN-Zielserver abhören bzw. verändern. Die unbefugten Personen können sowohl im BelWü und LVN sitzen als auch beim Leitungsbetreiber des BelWü bzw. LVN.
Maßnahmen: Nummer 13, 14, 15
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: gering.

Das Restrisiko besteht zum einen darin, dass sich der PC-Nutzer nicht an die (weiter unten aufgeführten) Vorgaben hält bzw. dass er Viren/trojanische Pferde aus dem Internet herunterlädt (z.B. BackOrifice, das eine Hintertür auf dem PC eröffnet). In die erste Kategorie fällt z.B. die mangelhafte Pflege des PCs. In die zweite Kategorie fallen z.B. Viren, Java- und Active-X Programme.
Maßnahmen: Nummer 11, 12
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: mittel.

3.1.3 Maßnahmenkatalog

Zum Schutz des PC vor unbefugtem Zugriff sind folgende Maßnahmen zu ergreifen:

1. Der PC darf nur mit einem Netzwerkinterface betrieben werden, d.h. z.B. Modem oder ISDN-Karte sind nicht zulässig.

2. Der PC muss in einem abschliessbaren Raum stehen. Der Raum darf durch Unbefugte nicht zu betreten sein.

3. Der PC muss regelmäßig mittels eines aktuellen Virencheckprogramms überprüft werden.

4. Der Einsatz einer Personal Firewall auf dem PC wird empfohlen.

5. Der PC muss mit einem Boot-Passwort betrieben werden.

6. Der PC muss mit einem Betriebssystem betrieben werden, der eine Benutzerauthentifizierung mittels Passwort erlaubt (z.B. Windows NT, Windows XP Professional, Linux). Es dürfen nur Benutzer auf dem PC zugelassen werden, die diesen PC für den Zugang zum LVN nutzen.

7. Bei der Verbindung zwischen PC und VPN Konzentrator wird mittels "split tunnelung" erzwungen, dass während der Verbindung zum ZKD der PC keine Verbindung in das öffentliche Internet hat. "split tunnelung" wird durch eine entsprechende Konfiguration im VPN Konzentrator erzwungen.

8. PC-Passwörter müssen sicheren Vorgaben hinsichtlich Länge/Form/Gültigkeitsdauer/etc. genügen. Es dürfen nicht dieselben Passwörter für die LVN-Anwendung benutzt werden wie für Anwendungen im LAN.

9. Der PC muss mit einem passwortgeschütztem Bildschirmschoner betrieben werden, der nach einer kurzen Zeit der Nutzerinaktivität erneut das Passwort verlangt.

10. Der PC muss eine sichere Version der VPN Client-Software benutzen - d.h. sobald sicherheitskritische Fehler in der VPN Client-Software bekannt werden, muss sie umgehend auf eine sichere Version erneuert werden.

11. Der PC-Nutzer ist hinsichtlich der Sicherheitsgefahren entsprechend zu schulen.

12. Der Sicherheitsbeauftragte der Einrichtung hat in regelmäßigen Abständen die Einhaltung der obigen Schutzmaßnahmen zu kontrollieren.

Zum Schutz der Datenverbindung zwischen PC des BelWü-Teilnehmer und dem LVN sind folgende Maßnahmen zu ergreifen:

13. Die unverschlüsselte Verbindung zwischen Cisco1605, Web-Proxy und VPN Konzentrator darf nur in einem abgeschlossenen Datenschrank in einem abgeschlossenen Rechenzentrumsraum erfolgen. Der Datenschrank darf nicht durch den Standardschlüssel zu öffnen sein; der Zugang soll stattdessen durch einen Zahlencode erfolgen.

14. Der Tunnel für die Datenkommunikation zwischen dem PC des BelWü-Teilnehmer und dem VPN Konzentrator ist mittels IPSec zu verschlüsseln. Dasselbe gilt für den Tunnel zwischen dem Cisco1605 des VPN Konzentrator und dem Cisco2691 beim LVN. Es wird ein 56 bit Schlüssel (DES) als ausreichend angesehen. Bei Bedarf kann auch ein 128 bit Schlüssel (3DES) verwendet werden.

15. Der Kommunikationsweg zwischen PC und VPN Konzentrator sowie zwischen Cisco1605 und Cisco2691 soll primär über geschützte Backbonestrecken bzw. geswitches LANs gehen.

16. Accesslisten auf dem Web-Proxy und dem Cisco1605 erlauben nur PC/Server Verbindungen, die auf den genutzten Port eingeschränkt werden. Der Verbindungsaufbau zwischen PC und VPN Konzentrator ist durch individuelle Usernamen und Passwörter geschützt.

17. Konfigurationsänderungen des Cisco2691, Cisco1605, Web-Proxy und VPN Konzentrator durch unbefugte Dritte werden durch Passwörter und entsprechende Zugangsaccesslisten verhindert, die einen Zugriff nur durch die BelWü-Koordination gewähren.

3.2 Phasenkonzept Realisierung

Die Nutzung des Web-Proxy ist bei Bedarf auf neue, unkritische Dienste im LVN zu erweitern.

3.3 Regelungen (technisch und organisatorisch)

3.3.1 Maßnahmen PC-Nutzer

- Bereitstellung/Konfiguration/Wartung des PCs.
- Einhaltung der Sicherheitsregeln hinsichtlich des Betrieb des PCs.

3.3.2 Maßnahmen BelWü

- Konfiguration/Bereitstellung/Wartung des Cisco1605, VPN Konzentrator und Web-Proxy.
- Konfiguration/Bereitstellung/Wartung des Cisco2691.

3.3.3 Maßnahmen ZKD/LVN

Zusätzliche Sicherheit kann am LVN-Firewall durch Filterung mit geeigneten Access-Listen erzielt werden. Eine zusätzliche Verschlüsselung auf Anwendungsebene (z.B. SSL, ssh) minimiert das Sicherheitsrisiko nochmals.

3.3.4 Technische Standards

Für die Kommunikationsverbindung zwischen dem Cisco1605 und dem Cisco2691 beim LVN wird als Protokoll nur IPSec verwendet. Dasselbe gilt für die Verbindung zwischen PC und Web-Proxy. Innerhalb dieses IPSec Tunnels können bei Bedarf alle TCP/IP Protokolle verwendet werden.
Aus Gründen der zusätzlichen Sicherheit ist eine Anwendungsverschlüsselung mittels https bei webbasierenden Zugängen vorzunehmen. Die tatsächlich verwendeten Protokolle orientieren sich an den im LVN zugelassenen Anwendungen.

Kapitel 4

Änderungshistorie

Version	Datum	Änderungen
0.9	20.01.2003	Erster Entwurf
1.0	09.07.2003	Zusätzliche Ziele MSWEB, www.nsi.bwl.de und www.on-demand.bwl.de

Kapitel 5

Verwendete Abkürzungen / Begriffe

3DES	triple Data Encryption Standard (Verschlüsselungsverfahren)
AH	Authentication Header (Internet Protokoll zur Authentifizierung)
BackOrifice	Fernwartungsprogramm für Windows-PCs (trojanisches Pferd von Hackern)
BelWü	Baden-Württembergs extended lan (Landeshochschulnetz)
BRI	Basic Rate Interface (ISDN-Schnittstelle)
BSI	Bundesamt für Sicherheit in der Informationstechnik
Cisco	Routerhersteller
DES	Data Encryption Standard (Verschlüsselungsverfahren)
DIPSY	Dialogorientiertes Personalverwaltungssystem (Personalinformationssystem des LBV)
DV	Datenverarbeitung
EPVS	Einheitliches Personalverwaltungssystem
FAT32	File Allocation Table (Dateisystem für Microsoft Windows)
GRE	Generic Routing Encapsulation (Internet Protokoll für Tunnel)
HTTP	Hypertext Transport Protocol (Internet Protokoll)
HTTPS	Hypertext Transport Protocol mit SSL-Sicherheitstechnik (Internet Protokoll)
IP	Internet Protocol (Internet Protokoll der Schicht 3)
IP Spoofing	Vortäuschung fremder IP-Adressen
IPSec	verschlüsseltes IP
ISAKMP	Internet Security Association and Key Management Protocol (Internet Protokoll)
LAN	Local Area Network
LBV	Landesamt für Besoldung und Versorgung Baden-Württemberg
LZP	Logistikzentrum der Polizei
LIS	Landesinformationssystem
LVN	Landesverwaltungsnetz in Baden-Württemberg
LVN-ID	Landesintranet-Server des LVN
LWL	Lichtwellenleiter

MLR	Ministerium Ländlicher Raum
MSWEB	Zusammenarbeit zwischen Microsoft und dem Land Baden-Württemberg
MWK	Ministerium für Wissenschaft, Forschung und Kunst
NSI	Neues Steuerungs-Instrument
NTFS	NT Filesystem
PGP	Pretty Good Pricacy (E-Mail Verschlüsselungsverfahren)
RUS	Rechenzentrum der Universität Stuttgart
SMTP	Simple Mail Transfer Protocol (Internet Anwendungsprogramm)
SNA	Systems Network Architecture (IBM Netzwerk)
SSL	Secure Socket Layer (Internet-Sicherheitstechnik)
StaLA	Statistisches Landesamt
TCP	Transmission Control Protocol (Internet Protokoll)
UVM	Ministerium für Umwelt und Verkehr
VLAN	Virtuelles LAN
VPN	Virtuelles Privates Netz
ZfI	Zentrum für Informationsverarbeitung der Finanzverwaltung Baden-Württemberg
ZKD	Zentrum für Kommunikationstechnik und Datenverarbeitung Baden-Württemberg