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 Einzelplatz-PC
V 2.0 vom 10.7.2003

Inhaltsverzeichnis

Kapitel 1

Einleitung

Der Zweck dieses Papiers ist die Darstellung eines sicheren und kostengünstigen Zugangs von BelWü-Teilnehmern zu LVN-Diensten. Dies erfolgt über einen LVN-Einzelplatz-PC, der mittels eines verschlüsselten Kanals (VPN) angebunden wird - sicherheitstechnisch entsprechend einer ISDN-Karte im PC.

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 hier vorliegenden ersten Stufe wird der Zugang mittels LVN-Einzelplatz-PC beschrieben; in einer folgenden Stufe wird der Zugang mittels LAN behandelt. Im vorliegenden Papier wird anwendungsseitig EPVS, NSI, LIS und Literaturdatenbank erläutert. Hinsichtlich Mail wird in dieser ersten Stufe kein Bedarf gesehen, da der LVN-Einzelplatz-PC eine zweite Mailbox des Benutzers bedeuten würde und kein Bedarf für einen datenschutzrelevanten Mailaustausch über den LVN-Einzelplatz-PC besteht. Mail sollte im Zusammenhang der zweiten Stufe und der Einbindung in das Mailsystem der Einrichtung behandelt werden - insbesondere im Rahmen des Pilotversuches des ZKD mit Mailtrust. Bei einem weiteren Bedarf von zusätzlichen Anwendungen oder veränderten Betriebsbedingungen wird das Konzept fortgeschrieben. Dies umfasst neben der Mail z.B. die BW-Card, anwendungsbasierende Ende-zu-Ende-Verschlüsselung sowie digitale Unterschriften sobald LVN-seitig die notwendigen Voraussetzungen geschaffen sind.

Das vorliegende BelWü/LVN Sicherheitskonzept der ersten Stufe soll als Musteranweisung für kleinere Einrichtungen dienen, die an das LVN angeschlossen werden möchten. Diese müssen einen entsprechenden formlosen Antrag an die BelWü-Koordination (ip@belwue.de) stellen.

Kapitel 2

Wirtschaftlichkeitsberechnung

Die Kosten der angestrebten Sammellösung für 50 bis 100 BelWü-Teilnehmer sind im Vergleich zur konventionellen LVN-III Anbindung wesentlich geringer:

Bei der angestrebten Sammellösung treten keine Leitungskosten auf, da die MWK / ZKD Leitung, die zur Internetanbindung des LVN dient, problemlos mitgenutzt werden kann. Auf Seiten der MWK-nachgeordneten Einrichtungen treten Hardwarekosten (Cisco1605 mit je 1250.- Euro) auf. Bei ca. 100 Einrichtungen wären die Gesamtkosten 125.000 Euro einmalig.

Bei der konventionellen LVN-III Anbindung treten pro MWK-nachgeordneter Einrichtungen ca. 450.- Euro/Monat für einen 128 KBit/s LVN-III managed Port auf (ca. 1250 Euro/Monat bei 2 MBit/s). Bei ca. 100 Einrichtungen wären die Gesamtkosten 45.000 Euro monatlich (bei 128 KBit/s Ports).

Der PC ist bei beiden Lösungen notwendig. Von Seiten des ZKD wird nach derzeitigem Stand der Aufwand beim ZKD für die beiden Lösungen als vergleichbar 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:

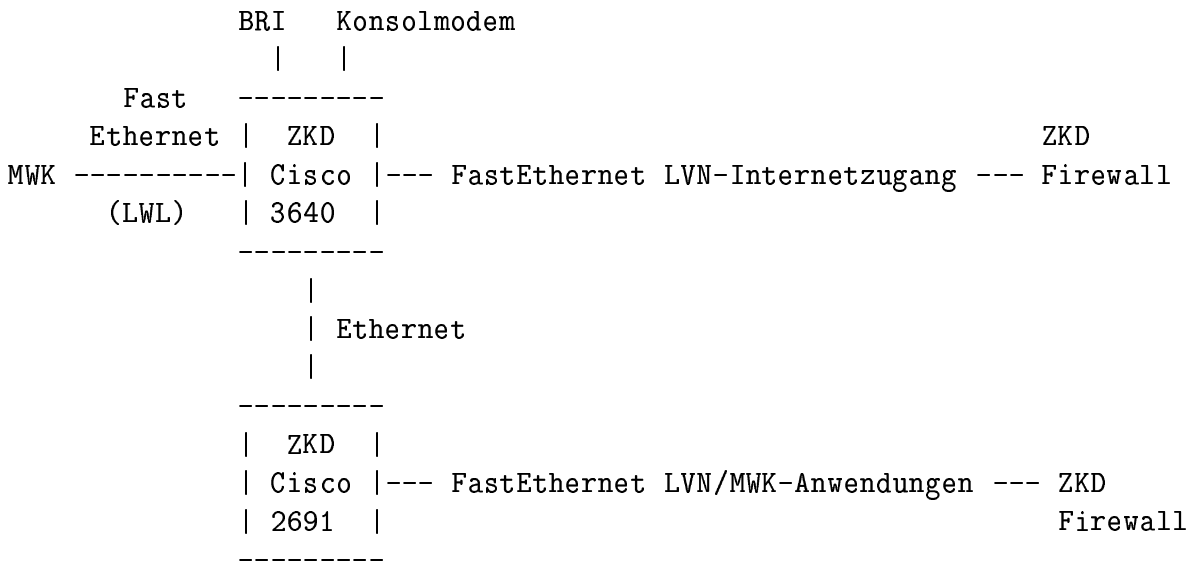
- Mailaustausch über das öffentliche Internet (per SMTP).
- Zugang zu LVN-Anwendungen wie DIPSY über einen IPSec Tunnel zwischen LVN und Einzelplatz-PC über BelWü.
- Zugang zu LVN-Anwendungen wie NSI über einen IPSec Tunnel zwischen LVN und LAN einer BelWü-Hochschule.

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.

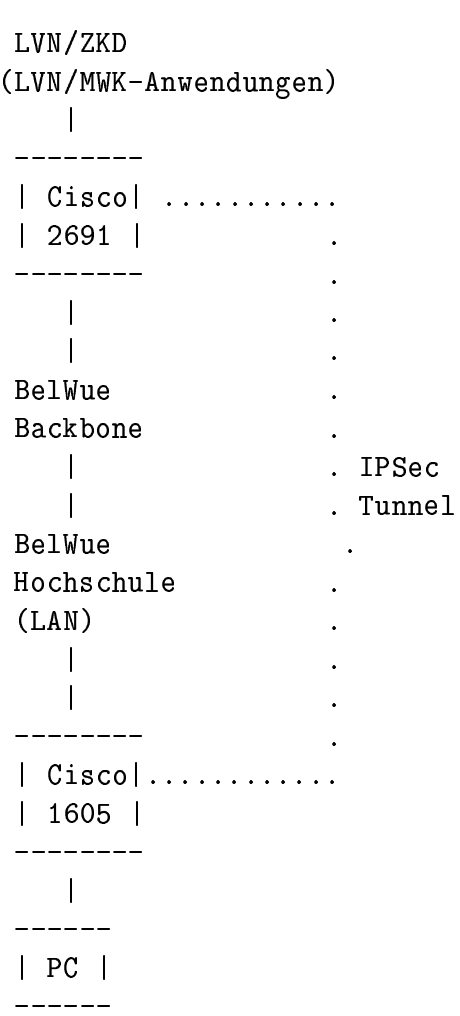


Um die Zuständigkeiten zwischen BelWü und LVN besser abzugrenzen, wurde in Absprache mit dem ZKD der Cisco3640 mit drei Ethernetinterfaces beim ZKD installiert. Dadurch ergeben sich zwei Ethernetinterfaces zum ZKD - eins für den (öffentlichen) Internetzugang des LVN und das andere für die LVN/MWK-Anwendungen (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 einen LVN-Einzelplatz-PC mit seperatem Router



Diese Anbindung stellt den sichersten Zugang dar, der einem PC mit ISDN-Karte zum LVN entspricht.

Der IP-Tunnel wird hier von einem Router (benötigt mindestens zwei Ethernet-Interface, vorzugsweise Cisco1605), an dem der auf das LVN zugreifende Arbeitsplatzrechner hängt, aufgebaut. Der PC verwendet IP-Adressen aus 10.15.0.0/16 bzw. 10.16.0.0/16. Der LVN-Einzelplatz-PC hat keinen zusätzlichen Zugang ins öffentliche Internet. Andernfalls könnte z.B. durch ein zweites Ethernet-Interface und mittels geeigneter Software (wie z.B. BackOrifice) eine Zugriffsmöglichkeit auf das LVN durch unberechtigte Dritte entstehen.

Vorteil des Konzeptes ist, dass es zu keinen Inkompatiblitäten zwischen Firewall-Software und Cisco-Betriebssystem bei der Tunnelkonfiguration kommen kann. Der Cisco-Router wird von der BelWü-Koordination konfiguriert und betreut. Dadurch

kann eine kleinere Organisation (Einzelplatzrechner z.B. in einem Fachbereich einer Hochschule) an das LVN mit ausreichender Sicherheit angebunden werden, da keine Firewallsoftware von einem lokalen Administrator konfiguriert und betreut werden muß.

Nachteile dieses Systems sind die Nichtverfügbarkeit des Internet auf dem PC, die fehlende Einbindung in die Bürokommunikation der Einrichtung sowie die zusätzlichen Kosten bei einem zweiten Einzelplatz-PC (bei einem zweiten Cisco1605) innerhalb derselben Hochschulverwaltung.

Aus Kostengründen werden ab Version 1.1 dieses Sicherheitskonzeptes folgende Erweiterungen zugelassen:
An einen Cisco1605 können unter bestimmten Voraussetzungen mehrere LVN-Einzelplatz-PCs angeschlossen werden. Diese sind mittels eines Ethernetswitches untereinander und dem Cisco1605 verbunden.
Ein PC kann unter bestimmten Voraussetzungen als Dual Boot System betrieben werden. Dadurch kann derselbe PC als normaler Arbeitsplatzrechner benutzt werden bzw. nach einem Neustart unter einer anderen Betriebspartition als LVN-Einzelplatz-PC.
Der LVN-Einzelplatz-PC kann direkt an einen Ethernetport des normalen BelWü IP-Produktions-Routers der Hochschule angeschlossen werden, sofern dort ein Ethernetport frei ist.

Aus Kostengründen wird ab Version 1.2 dieses Sicherheitskonzeptes folgende Erweiterung zugelassen:
An einen Cisco1605 können unter bestimmten Voraussetzungen mehrere LVN-Einzelplatz-PCs angeschlossen werden. Diese sind mittels eines VLAN untereinander und dem Cisco1605 verbunden.

Aus Kostengründen wird ab Version 2.0 dieses Sicherheitskonzeptes folgende Erweiterung zugelassen:
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.

3.1.2 Risikobewertung

3.1.2.1 Bedrohungsanalyse

Hinsichtlich der Bedrohung muss unterschieden werden, ob der LVN-Einzelplatz-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 11, 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 isoliert vom LAN betrieben wird und die Kommunikation zwischen PC und Server mittels IPSec verschlüsselt wird. Da der PC allerdings Zugriff auf "interessante" Anwendungen beim LVN hat, stellt der PC ein potentielles Angriffsziel dar, für das entsprechende (weiter unten aufgeführte) Maßnahmen zu ergreifen sind.
Maßnahmen: Nummer 1 bis 13, 16
Risikobewertung hinsichtlich des Auftretens: sehr gering.
Risikobewertung hinsichtlich des Schadens: groß.

Ein weiteres Risko besteht in dem Ethernetkabel zwischen dem PC des BelWü-Teilnehmers und dem Cisco1605, über den die Datenkommunikation unverschlüsselt erfolgt. Da dieses Kabel sehr kurz ist und nicht öffentlich zugänglich ist, wird dieses Risiko als sehr gering betrachtet.
Maßnahmen: Nummer 2

Risikobewertung hinsichtlich des Auftretens: sehr gering.
Risikobewertung hinsichtlich des Schadens: groß.

Im Fall von mehreren LVN-Einzelplatz-PCs hinter dem Cisco1605 besteht das Risiko, dass die unverschlüsselte Datenkommunikation zwischen den PCs abgehört wird.
Maßnahmen: Nummer 3
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: groß.

Im Fall von mehreren LVN-Einzelplatz-PCs hinter dem Cisco1605, die mittels VLAN verbunden sind, besteht das Risiko, dass ein LVN-Einzelplatz-PC angegriffen wird. Dies kann durch die Komprimitierung des VLAN-Switches erfolgen oder indem im Patchfeld ein LVN-Einzelplatz-PC durch einen anderen komprimitierten PC ersetzt wird.
Maßnahmen: Nummer 4
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: groß.

Im Fall der (wirtschaftlichen) Nutzung eines PCs sowohl als normalem Arbeitsplatzrechner sowie nach einem Neustart unter einer anderen Betriebssystempartition als LVN-Einzelplatz-PC besteht das Risiko, dass ein Einbruch in den normalen Arbeitsplatzrechner die Integrität der LVN-Einzelplatz-PC Betriebssystempartition beeinträchtigt. Ohne Risiko ist hingegen die Nutzung eines Tastatur- und Bildschirmumschalters bei der Nutzung von zwei getrennten PCs (aber mit gemeinsamer Tastatur/Bildschirm).
Maßnahmen: Nummer 7
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: groß.

Ein weiteres Risiko besteht darin, dass unbefugte Personen durch Konfigurationsänderungen des Cisco1605 bzw. Cisco2691 Zugriff auf die übermittelten Daten erhalten bzw. Zugang zum LVN erhalten. Die Auswirkungen des letzteren Risikos kann durch zusätzliche Accesslisten auf dem LVN-Firewall minimiert werden.
Maßnahmen: Nummer 17
Risikobewertung hinsichtlich des Auftretens: sehr gering.
Risikobewertung hinsichtlich des Schadens: groß.

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: gering.

Ein weiteres Risko besteht darin, dass unbefugte Personen den Datenverkehr inner-

halb 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 14, 15, 18 bis 21
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: groß.

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 von einem LVN-Server herunterlädt (z.B. BackOrifice, das eine Hintertür auf dem PC eröffnet). In die erste Kategorie fällt z.B. der Einbau einer zweiten Ethernetkarte, damit der PC-Nutzer den Rechner auch für andere Zwecke in seinem LAN oder Internet nutzen kann. In die zweite Kategorie fallen z.B. Viren, Java- und Active-X Programme. Im ersten Fall muss der Nutzer entsprechend geschult werden; im zweiten Fall wird das Risiko von fragwürdigen Downloads von LVN-Servern als sehr gering angesehen.
Maßnahmen: Nummer 12, 13
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: mittel bis groß.

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 zusammen mit dem Cisco1605 in einem abschließbaren Raum stehen. Der Raum darf durch Unbefugte nicht zu betreten sein.

3. Verbindungen zwischen mehreren LVN-Einzelplatz-PCs müssen über einen extra Ethernetswitch sowie eine eigene Kabelinfrastruktur erfolgen. Ein VLAN über die allgemeine Kabelinfrastruktur erfordert zusätzliche Maßnahmen. Falls die eigene Kabelinfrastruktur mittels Kabelpatchungen erreicht wird, dürfen die Patchfelder durch Unbefugte nicht erreichbar sein.

4. Das remote Management zum VLAN Switch muss sicher sein (kontrollierter Zugang durch eine restriktive Accessliste, sichere Passwörter).
   Zwischen lokalem LVN-Einzelplatz-PC und lokalem Cisco1605 muss bei Einsatz eines VLAN ein IPSec Tunnel verwendet werden.
   Der Zugang zu beteiligten Patchfeldern und Switchen muss vor dem Zugriff Unbefugter gesichert sein.

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

6. Der PC muss mit einem Betriebssystem betrieben werden, das 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 Dual Boot Systemen wird der optimale Schutz geschaffen, wenn die beiden Betriebssysteme nicht auf derselben Festplatte liegen, sondern über Wechselmedien bereitgestellt werden. Falls dies nicht möglich ist, darf von der Partition des normalen Arbeitsplatzrechners nicht auf das Filesystem der Partion des LVN-Einzelplatz-PCs lesend oder schreibend zugegriffen werden. Unter Microsoft Betriebssystemen kann dies z.B. realisiert werden, indem der LVN-Einzelplatz-PC NTFS (z.B. unter Windows NT) und der Arbeitsplatzrechner FAT32 (z.B. unter Windows 95, Windows 98, Windows ME) verwendet. Besonders wichtig bei Dual Boot Systemen ist insbesondere die Einhaltung der Maßnahme 1 (nur eine Ethernetkarte im Rechner).

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 darf nicht zum "surfen" im öffentlichen Internet mittels des Web-Proxy des LVN benutzt werden (Gefahr von Viren/trojanische Pferde).

11. Auf dem PC darf außer der LVN-Anwendungssoftware (notwendige Software für den LVN-Betrieb, z.B. Office-Anwendungen, sonstige Zusatzprogramme) keine weitere zusätzliche Anwendungssoftware installiert sein. Diese Software darf ausschließlich für den LVN-Betrieb genutzt werden.

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

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

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

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

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

16. Eine Accessliste auf dem Cisco1605 beim PC des BelWü-Teilnehmer erlaubt nur PC/Server Verbindungen, die auf den genutzten Port eingeschränkt werden.

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

3.1.3.1 EPVS

Der Datenaustausch im Zusammenhang mit EPVS, z.B. DIPSY, wird durch die oben aufgeführten Maßnahmen als ausreichend sicher betrachtet. DIPSY ist eine Dialoganwendung und benutzt auf dem PC des BelWü-Teilnehmers einen java-basierenden Web-Client. Hierfür wird derzeit http (Port 80) sowie die Ports 1098 und 1099 verwendet. LBV-seitig ist ein Betrieb über https mit Vorlauf von ca. einer Woche möglich. Ein Nachteil von https ist ein größeres Datenvolumen, welches aber als akzeptabel erscheint. Der Zugangs-Webserver steht im ZKD, der Anwendungshost im ZfI. Zwischen den beiden Rechnern geht der Verkehr unverschlüsselt über das LVN. Bei Bedarf kann eine Verschlüsselungsbox zwischen ZKD und ZfI eingesetzt werden (Kostenbedarf ca. 20.000.- EURO). Das ZKD kann bei der Beschaffung eines SSL-Zertifikats behilflich sein. BW-Card Unterstützung ist prinzipiell möglich.

Zum Schutz der Datenverbindung der EPVS-Anwendung sind folgende Maßnahmen zu ergreifen:

18. Als Übertragungsprotokoll ist https anstelle von http zu verwenden.

19. Der Einsatz der BW-Card ist vorzusehen, sobald diese verfügbar und anwendbar ist.

3.1.3.2 NSI

Der Datenaustausch im Zusammenhang mit NSI wird durch die oben aufgefürten Maßnahmen als ausreichend sicher betrachtet. NSI ist eine webbasierende Anwendung. Als Übertragungsprotokoll ist https geplant. Eine BW-Card Unterstützung ist von Seiten des NSI in der Überlegung. Der Standort des NSI Servers ist beim BDZ in Göppingen. Der Zugang der meisten Hochschulverwaltungen erfolgt über einen Rechner bei der Planungsgruppe (PLGR) Reutlingen.

Zum Schutz der Datenverbindung der NSI-Anwendung sind folgende Maßnahmen zu ergreifen:

20. Als Übertragungsprotokoll ist https zu verwenden.

21. Der Einsatz der BW-Card ist vorzusehen, sobald diese verfügbar und anwendbar ist.

3.1.3.3 LIS, Literaturdatenbank beim StaLA

Bei der Kommunikation eines per IPSec und Cisco1605 an das LVN angebunden PC eines BelWü-Teilnehmers mit LIS sind neben den obigen Maßnahmen 1 bis 12 keine weiteren Maßnahmen mehr erforderlich.
Da die Literaturdatenbank beim StaLA keine sicherheitskritische Anwendung darstellt, ist u.E. sogar die Sicherheitsanforderungen an den BelWü-Teilnehmer noch geringer: Es sollte ein Cisco1605 mit IPSec Tunnel mit entsprechender Accessliste ausreichend sein; der PC kann u.E. sogar eine zweite Netzwerkkarte im LAN des BelWü-Teilnehmers besitzen.

3.1.3.4 LVN-ID, Vorschriftendienst, Fortbildung 21, MSWEB, NSI-Informationen und Büroshop des LZP

Bei der Kommunikation eines per IPSec und Cisco1605 an das LVN angebunden PC eines BelWü-Teilnehmers mit LVN-ID (Landesintranet-Server; 10.127.255.100, Port 80), Vorschriftendienst Baden-Württemberg (www.vd-bw2.bwl.de; 10.127.255.35 und 10.127.255.36, Port 80), Fortbildung 21 (www.fobi21.bwl.de; 10.127.255.111, Port 80), NSI-Informationen (www.nsi.bwl.de, 10.125.248.17 und www.nsi-online.bwl.de, 10.127.255.112 und www.on-demand.bwl.de, 10.125.237.12; alle Port 80), MSWEB (Zusammenarbeit zwischen Microsoft und dem Land B-W; 10.127.255.140, Port 80) bzw. Büroshop des LZP (Logistikzentrum der Polizei; 10.127.255.62, Port 80; inzwischen auch über das öffentliche Internet unter www.shop.lzp.de erreichbar) sind neben den obigen Maßnahmen 1 bis 13 keine weiteren Maßnahmen mehr erforderlich.
All diese Dienste sind auf den Cisco1605 grundsätzlich immer zugelassen. Zusätzlich besteht seit Version 2.0 dieses Sicherheitskonzeptes auch die kostengünstige Möglichkeit, auf obige Dienste von einem normalen Arbeitsplatz mittels VPN Clientensoftware über einen BelWü-Web-Proxy zuzugreifen. Hierzu existiert ein eigenes Sicherheitskonzept.
Ab Version 2.0 dieses Sicherheitskonzeptes werden auf den Cisco1605 Zugriffe auf das gesamte ZKD Servernetz 10.127.254.0/23 freigeschaltet, da sich durch die zunehmende Anzahl der erreichbaren Server und die Anzahl der Cisco1605 der Pflegeaufwand stark erhöht hat. Auf dem IPSec-Tunnelendpunkt beim ZKD (Cisco2691) wird hingegen per Accessliste der Zugriff nur auf bestimmte IP-Adressen und Portnummern zugelassen.

3.2 Phasenkonzept Realisierung

Zwischen Version 1.0 und 1.1 dieses Papiers wurde die Bandbreite der Verbindung ZKD/BelWü von 2 auf 100 MBit/s erhöht. Außerdem wurde der Cisco3640, der den Endpunkt der IPSec Tunnel darstellt, vom RUS zum ZKD verlegt. Zwischen Version 1.2 und 2.0 wurde der Cisco2691 beim ZKD installiert.

3.3 Regelungen (technisch und organisatorisch)

3.3.1 Maßnahmen BelWü-Einrichtung

- Installation des Routers im LAN vor dem PC nach Vorgaben der BelWü-Koordination.
- Bereitstellung/Konfiguration/Wartung des PCs.
- Einhaltung der Sicherheitsregeln hinsichtlich des Betrieb des PCs.

3.3.2 Maßnahmen BelWü

- Konfiguration/Bereitstellung/Wartung des Cisco1605.
- 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. DIPSY) minimiert das Sicherheitsrisiko nochmals.

3.3.4 Technische Standards

Für die Kommunikationsverbindung zwischen dem Cisco1605 beim PC des BelWü-Teilnehmer und dem Cisco2691 beim LVN wird als Protokoll nur IPSec verwendet. Innerhalb dieses IPSec Tunnels können bei Bedarf alle TCP/IP Protokolle verwendet werden. Wenn der Cisco1605 hinter einer Firewall beim BelWü-Teilnehmer sitzt, müssen dort folgende Protokolle reigeschaltet sein: GRE (IP Protokoll 47), AH (IP Protokoll 51) und ISAKMP (UDP Port 500).

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	8.8.2000	Erster Entwurf
0.91	10.8.2000	EPVS/NSI ausführlicher, Mail als Anwendung entfernt, diverse Ergänzungen/Korrekturen
1.0	21.8.2000	Stufenkonzept
1.1	20.2.2002	Update Netzanbindung (100 statt 2 MBit/s zum ZKD, Cisco3640 beim ZKD); mehrere PCs hinter dem Cisco1605; dual-boot PC; PC am BelWü-Hauptrouter; LVN-ID, MSWEB und LZP-Büroshop, u.a.
1.2	21.3.2002	mehrere PCs über VLAN hinter einem Cisco1605
1.11	15.1.2003	Anwendungssoftware für LVN-Anwendungen
2.0	10.7.2003	10.127.254.0/23 auf den Kundenroutern freigeschalten; Cisco2691 beim ZKD; Cisco831 anstelle Cisco1605; 3DES; Vorschriftendienst, Fortbildung 21, NSI-Informationen; NSI-Zugang über PLGR Reutlingen; IPSEC-Protokolle; alternativer Zugang über Web-Proxy

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