Schweizerische Organisation für Geo-Information
Organisation Suisse pour l'Information Géographique
Organizzazione Svizzera per l'Informazione Geografica
Swiss Organisation for Geographic Information

SICHERHEITSASPEKTE BEI GIS-WEB LÖSUNGEN

Bericht der Fachgruppe GIS-Technologie SOGI

28.03.2004

Autoren:
- Urs Flückiger, ESRI Geoinformatik AG, Zürich (Leiter)
- Dominik Angst, ITV Geomatik AG, Regensdorf
- Wolfgang Bühler, SCB Digital AG, Lenzburg
- Rolf Eugster, F+P Geoinfo AG, Herisau
- Matthias Liechti, C-Plan AG, Gümligen
- Erwin Sägesser, Intergraph (Schweiz) AG, Dietikon
- Prof. Stefan F. Keller, Hochschule für Technik Rapperswil
- Dirk Burghardt, Geographisches Institut Universität Zürich

Inhaltsverzeichnis

1 EINLEITUNG 3

2 WAS IST SICHERHEIT? 4

2.1 Definition Sicherheit 4

2.2 Risikoanalyse 5

3 SICHERHEITSPROZESS 7

3.1 Gefährdungen 7

3.2 Vorgehensweise zur Risikoanalyse 9

3.3 Inhalte und Begriffe zum Sicherheitskonzept 9

4 LÖSUNGSKOMPONENTEN UND TECHNOLOGIEN 11

4.1 Grundanforderungen 11

4.2 Komponenten einer GIS-Web-Lösung 12

4.3 Technologien 14

5 SZENARIEN, ANWENDUNGSBEISPIELE UND KONFIGURATIONSBEISPIELE AUS DEM GIS-BEREICH 23

5.1 Szenario 1: Datenherr betreibt Daten-Server selber 23

5.2 Szenario 2: Datenprovider betreibt Daten-Server für Datenherrn 26

5.3 Szenario 3: Mehrere Datenherren betreiben gemeinsamen Daten-Server 30

5.4 Weitere Aspekte 33

6 ANHANG 36

6.1 Checklisten Sicherheit bei Web-Lösungen 36

6.2 Literatur 40

6.3 Glossar 41

6.4 Abkürzungen 43

1 Einleitung

Mit der rasanten Verbreitung des Internets und dessen Nutzung für private und geschäftliche Transaktionen treten Sicherheitsfragen immer stärker in den Vordergrund. Insbesondere für Unternehmen ist die Einführung einer zuverlässigen IT-Sicherheitspolitik heute unabdingbar. Der vorliegende Bericht beschäftigt sich deshalb ausführlich mit dem Thema der Sicherheitsfragen bei Web-Lösungen.

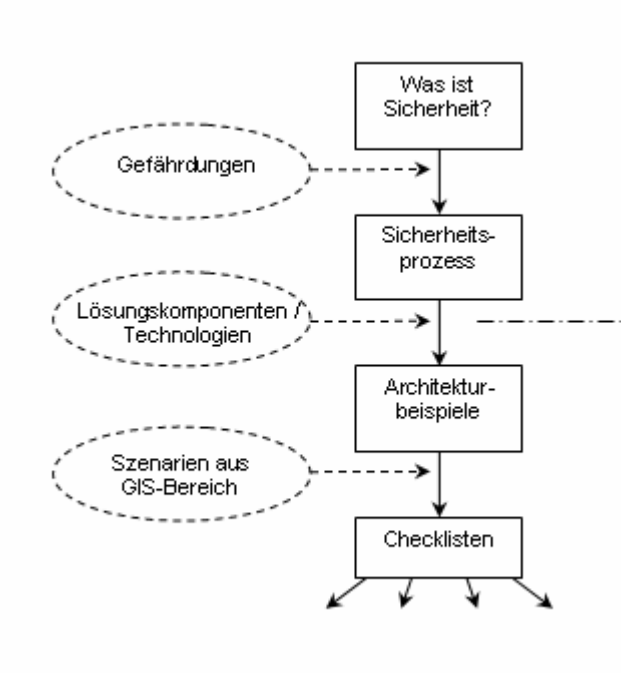


Abbildung 1: Schematische Darstellung des Berichtes

Nach einer kurzen Einführung zum Sicherheitsbegriff werden potentielle Gefahren und Möglichkeiten der Risikoanalyse vorgestellt. Diese bilden die Grundlage für die Auswahl angepasster Sicherungsmassnahmen, unter Berücksichtigung von Aufwand und Nutzen. Nach einer Beschreibung von Lösungskomponenten und mehreren Architekturbeispielen werden diese auf mögliche Szenarien aus dem GIS-Bereich angewendet. Der Bericht endet mit der Zusammenstellung einer Checkliste, welche ein Sicherheitsmanagement unter Berücksichtigung von Risikoveränderungen erlaubt, und einem Glossar, in welchem die wichtigsten Begriffe aufgeführt sind.

Der Bericht wurde von der Fachgruppe GIS-Technologie der Schweizerischen Organisation für Geo-Information (SOGI) verfasst. Eine ausführliche Präsentation erfolgt im Rahmen des Workshops - „Sicherheitsaspekte von (GIS) Web-Lösungen“ - an der GIS/SIT 2004.

2 Was ist Sicherheit?

Sicherheit im Internet wird meistens unter dem Gesichtspunkt technischer Lösungen betrachtet. Vielfach wird die Meinung vertreten, Sicherheit sei allein durch die Auswahl einer geeigneten Firewallsoftware zu erreichen.

Die 100 Prozent sichere Lösung. Kurze und sichere Anleitung für den täglichen Gebrauch:

" .. um die garantiert sicherste Sicherheitslösung zu erzielen, installieren Sie die Firewall zwischen der Netzwerkkarte oder dem Modem und der Buchse in der Wand. Setzen Sie den Schnabel der Firewall quer über das Netzwerk- oder Telefonkabel und drücken Sie die beiden Hebel fest zusammen. Sobald die Installation korrekt ist, erlöschen sämtliche Leuchtdioden und die Ventilatoren werden leise. Das lässt darauf schliessen, dass sich Ihr Computersystem in einem sicheren Zustand befindet..."

Eine absolute Garantie der Sicherheit wird es sehr wahrscheinlich nicht geben. Mit dem Bericht wird jedoch versucht, einen ganzheitlichen Lösungsansatz für Sicherheitsfragen bei Web-Lösungen vorzustellen. Zudem werden grundlegende Konzepte der Themen Sicherheit und Risikoanalyse vorgestellt.

2.1 Definition Sicherheit

Der Sicherheitsbegriff hat sich mit der Entwicklung und veränderten Nutzung des Internets gewandelt. In der Entstehungsphase der 70er Jahre standen vor allem militärische Aspekte wie Geheimhaltung und ständige Verfügbarkeit im Vordergrund. Mit dem Anschluss von amerikanischen Universitäten und Forschungseinrichtungen erfolgte eine Erweiterung des Nutzerkreises mit dem Bedarf eines freizügigen Zugriffs auf Daten und Kommunikationsdienste. Zu Beginn der 90er Jahre schliesslich änderte sich die Nutzung des Internets vom reinen Informations- und Marketinginstrument hin zur Plattform für kommerzielle Anwendungen (Home-Banking, Online-Shopping). Die heutige Nutzung ist gekennzeichnet durch eine hohe Anzahl an Nutzern ohne explizite Identifikation und eine Übertragung von Daten beliebigen Inhaltes, wodurch der Aufbau von geeigneten Sicherungslösungen unumgänglich wird.

Für Unternehmen versteht sich Sicherheit als Zustand, in dem Informationen vor, während und nach der Verarbeitung vor Beeinträchtigung und Verlust der *Vertraulichkeit, Integrität,* und *Verfügbarkeit* bewahrt werden. In offenen Netzen wie dem Internet muss darüber hinaus die *Authentifikation* von Benutzern, die *Zugriffskontrolle*, die *Verbindlichkeit* von Kommunikationsbezie-

hungen und bei Bedarf auch die *Anonymität* des Ursprungs von Informationen gewährleistet sein.

Die gesetzlichen Aspekte des Datenschutzes werden in diesem Bericht nicht erörtert. Datenschutz ist keine technische Lösung, welche die Daten schützt. Im Zentrum der Betrachtung stehen technische und allenfalls organisatorische Lösungen.

2.2 Risikoanalyse

Die Risikoanalyse bezweckt bedarfsgerecht, mit den zur Verfügung stehenden Mitteln eine maximale Schutzwirkung aufzuzeigen. Die Entwicklung von Sicherungsmassnahmen ist mit einem entsprechenden zeitlichen und finanziellen Aufwand verbunden. Deshalb ist es für jedes Unternehmen wichtig, ein an ihre Bedürfnisse angepasstes Verhältnis von Sicherheit und verbleibendem Restrisiko zu bestimmen. Die Summe aus Kosten für die Sicherheitsmassnahmen und Kosten durch mögliche Schäden wird als Gesamtkosten aufgeführt und kann durch jedes Unternehmen optimiert werden. In Abbildung 2 wird dieses Optimum am Tiefpunkt der Kurve für die Gesamtkosten erreicht.

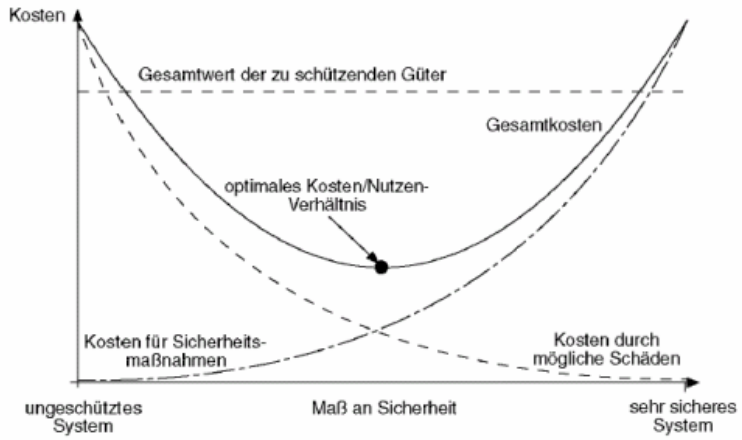


Abbildung 2: Verhältnis zwischen Aufwand an Sicherungsmassnahmen und verbleibendem Restrisiko

Für die Bestimmung der Risikofaktoren und zur Abschätzung des Restrisikos kann eine Risikoanalyse in 2 grundsätzlichen Ansätzen durchgeführt werden. Der erste Ansatz ergibt sich aus den Anforderungen an den Grundschutz oder durch eine detaillierte Analyse. Der Grundschutzansatz orientiert sich dabei in der Regel an vorhandenen Standards z.B. IT-Grundschutzhandbuch des deutschen Bundesamtes für Sicherheit in der Informationstechnik.

Das IT-Grundschutzhandbuch kann als Hilfsmittel bei der Konzeption, Realisierung und Revision von Standard-Sicherheitsmassnahmen verwendet werden. Um die verschiedenen Bereiche der Informationstechnologie zu be-

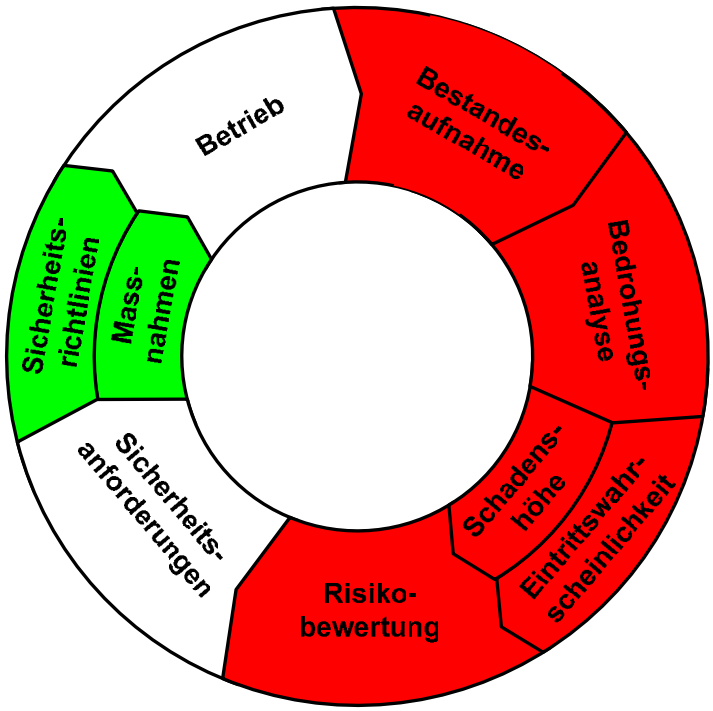
rücksichtigen, ist das IT-Grundschutzhandbuch in verschiedene Bereiche gegliedert. Die einzelnen Bausteine spiegeln typische Bereiche des IT-Einsatzes wieder, wie beispielsweise Client-Server-Netze, bauliche Einrichtungen, Kommunikations- und Applikationskomponenten. In jedem Baustein wird zunächst die zu erwartende Gefährdungslage beschrieben. Diese bildet die Grundlage, um ein spezifisches Massnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge zu generieren.

Der zweite Ansatz ist die detaillierte Risikoanalyse. Diese versucht alle Risiken möglichst vollständig zu erfassen und sie nach der potentiellen Schadenshöhe zu ordnen. Als Ansatz wird die mathematische Definition des Risikobegriffs verwendet, wobei sich Risiko als Produkt von Schadenshöhe und Eintrittswahrscheinlichkeit ergibt. Das Vorgehen zur Risikoabschätzung wird im folgenden Abschnitt detailliert erläutert.

3 Sicherheitsprozess

Sicherheit kann nicht in einem einmaligen Prozess definiert oder erlangt werden. Der Sicherheitsprozess versteht sich als eine zyklische Überprüfung der Sicherheitsmassnahmen und der zugrunde liegenden Gefährdungen.

Die nachfolgende Abbildung zeigt die Phasen eines Sicherheitskonzeptes. Der rote Bereich markiert den Teil der Risikoanalyse. Die restlichen Bereiche definieren die Sicherheitsanforderungen, die daraus abgeleiteten Richtlinien und Massnahmen sowie den eigentlichen Betrieb.



ROT: Risikoanalyse
GRÜN: Sicherheitskonzept

Abbildung 3: Phasen eines Sicherheitskonzeptes

3.1 Gefährdungen

Unternehmen sollten sich mit möglichen Gefahren vertraut machen, die eine IT-Infrastruktur mit sich bringt. Dies gilt vor allem dann, wenn man Geschäftstransaktionen mit Geschäftspartnern, Lieferanten und Kunden über das Internet abwickelt und die IT durch Schnittstellen zumindest teilweise öffnet. Grundsätzlich gibt es drei Gefahrenpotenziale: Nicht-autorisierter Zugriff auf vertrauliche Daten von aussen durch Hacker, Zugriff von innen durch unbefugte Mitarbeiter und Gefahren durch höhere Gewalt wie etwa Feuer.

Im Folgenden werden einige Varianten des missbräuchlichen (oder nicht-autorisierten) Zugriffs von aussen auf vertrauliche Daten vorgestellt.

Fall 1: Einbruch ins Netz

Hacker verwenden Portscanner um innerhalb kürzester Zeit Adressbereiche im Internet zu überprüfen. Bei Sicherheitslücken durch offene Ports können so Betriebssysteme, Serversoftware oder im schlimmsten Fall sensible Betriebsdaten gelesen werden. Wichtigstes Schutzmittel ist eine Firewall, die Datenpakete von außerhalb filtert oder abweist und das interne Netz nach außen hin abschirmt.

Fall 2: Download von Software

Mitarbeiter installieren Programme aus dem Internet. Diese können Viren oder Trojaner enthalten. Solche Schädlinge versuchen Daten zu zerstören, zu verändern, Daten an Fremde zu übermitteln oder sogar Zugriff auf den infizierten Rechner zu ermöglichen. Um so bekannten Trojanern wie „Back Orifice“ nicht zum Opfer zu fallen, sollte man nur vertrauenswürdige Adressen zum Download in betracht ziehen und auf jedem Computer eine aktuelle Viren-Software installieren.

Fall 3: Öffnen von E-Mail-Attachments

Seit dem "I LOVE YOU" Virus ist das Risiko bei angehängten Dokumenten an Emails nicht zu unterschätzen. Office Anwendungen wie z.B. Textdokumente oder Tabellenkalkulationsdateien bergen durch die Möglichkeit Makros einzubetten dieselbe Gefahrenquelle wie ausführbare Programme oder Scriptdateien. Mitarbeiter müssen auf den Umgang von Attachments sensibilisiert werden. Bei der Virensoftware sollte ein besonderes Augenmerk auf die Email-Attachment-Prüfung gelegt werden.

Fall 4: Aufrufen von Webseiten

Sicherheitslücken im Browserprogramm geben Angreifern die Möglichkeit auf die Festplatte des Computers zuzugreifen. Es sollten die aktuellen Sicherheitsupdates der Browserhersteller installiert sein. Dies sollte zentral über den Netzwerkadministrator gesteuert werden.

Fall 5: Social Engineering

Durch Vorspielen falscher Tatsachen verschicken Hacker Emails mit der Bitte, Passwörter und Benutzernamen bekannt zu geben. Solche manipulierten Emails sind für den Anwender nicht auf den ersten Blick zu erkennen. Bei vertraulichen Daten halten Sie telefonische Rücksprache mit dem vermeintlichen Absender. Durch schnelles Reagieren helfen Sie unter Umständen, grösseren Schaden abzuwenden.

Im LAN sind die Benutzer bekannt. Dennoch kann ein Nutzer sich unberechtigt ausweisen und so Zugang zu weiteren Bereichen sowie andere Rechte erlangen.

Fall 6: Abhörung

Ein Wireless Lan kann abgehört werden. Im sensitiven Bereich empfiehlt sich eine Verschlüsselung.

3.2 Vorgehensweise zur Risikoanalyse

Die Risikoanalyse setzt sich aus folgenden Punkten zusammen:

- Bestandsaufnahme
- Bedrohungsanalyse
- Eintrittswahrscheinlichkeit bestimmen, Schadenshöhe bestimmen
- Risikobewertung

Die Bestandesaufnahme erfasst alle schützenswerten Objekte des Unternehmens. Für jedes Objekt muss dabei dokumentiert werden, welche Bedrohungen bzw. Gefahren einen massgeblichen Einfluss auf die Geschäftstätigkeit und den laufenden Betrieb des Systems haben. Es kann dazu zwischen zufälligen Gefahren (Feuer, Wasser), menschlichem und technischem Versagen oder bewusst herbeigeführten Gefahren wie Manipulation oder Spionage unterschieden werden. Die Risikobewertung und alle daraus abgeleiteten Entscheidungen sind von der Abschätzung der Eintrittswahrscheinlichkeit und Schadenshöhe abhängig. Ergebnis ist eine Liste der einzelnen Risikopotentiale im Hinblick auf den Schaden aus finanzieller Sicht und der Abhängigkeit des Unternehmens von der Funktionsfähigkeit der untersuchten Systeme. Durch die Risikobewertung ergeben sich die konkreten Sicherheitsanforderungen für das Unternehmen. Diese bilden die Grundlage bei der Erstellung des Sicherheitskonzeptes.

3.3 Inhalte und Begriffe zum Sicherheitskonzept

Vordringliche Aufgabe des Sicherheitskonzeptes ist es, die in der Risikoanalyse identifizierten Sicherheitslücken durch geeignete Massnahmen zu schliessen. Ein umfassendes Sicherheitskonzept besteht dabei aus den drei folgenden Hauptkomponenten:

- Festlegung der Internet-Sicherheitsrichtlinien
- Beschreibung technischer Massnahmen (Sicherheitsarchitektur und Implementierungsvorschrift
- Beschreibung organisatorischer Massnahmen

Die Festlegungen der Internet-Sicherheitsrichtlinien sind unternehmensspezifisch und versuchen die im Rahmen der Risikoanalyse identifizierten Ressourcen eines Unternehmens zu schützen. Folgende Bereiche müssen in der Regel berücksichtigt werden:

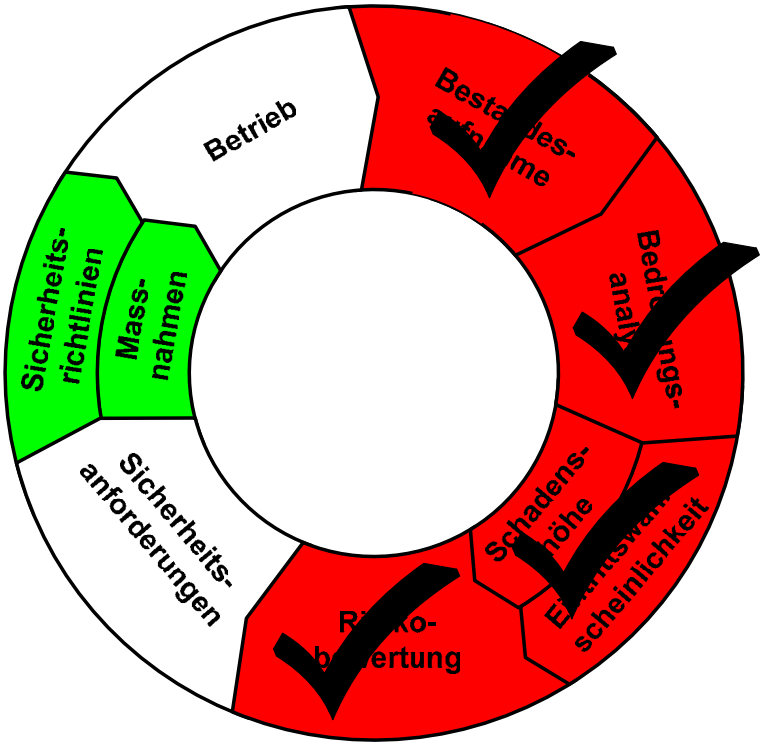
- Informationsklassifizierung und –kontrolle sowie der generelle Umgang mit vertraulichen Informationen

- Datensicherung und Lagerung von vertraulichen Daten
- Zugangskontrollen zu Gebäuden, Server-Räumen, Verteilerschränken etc.
- Diebstahlschutz
- Schulungsmaßnahmen für Mitarbeiter
- Regelungen im Umgang mit Verstößen gegen die Richtlinien (z. B. Disziplinarmaßnahmen)

Die getroffenen Massnahmen gehören den folgenden Kategorien an:

- Präventive Massnahmen - Firewall
- Überwachende Massnahmen – Logfiles, Intrusion Detection Systeme (IDS)
- Reaktive Massnahmen - Virenscanner

Aufgrund der geforderten Massnahmen muss eine entsprechende Architektur erstellt werden. Im Kapitel 4 werden die Komponenten beschrieben.



ROT: Risikoanalyse
GRÜN: Sicherheitskonzept

Abbildung 4: Abgeschlossene Risikoanalyse

4 Lösungskomponenten und Technologien

In den folgenden Kapiteln wird die Grundlage für die erfolgreiche Umsetzung des Sicherheitskonzeptes gelegt. Die Kapitel definieren und beschreiben Begriffe aus der Fachwelt. Auf diesem Werkzeugkasten aufbauend lassen sich später verschiedene Sicherheitsmodelle und Architekturen aufbauen. Zudem gibt die Einführung eine Grundlage für Gespräche mit Sicherheitsexperten oder Auftragnehmern.

Das Kapitel 4.1 "Grundanforderungen" beschäftigt sich mit Konzeptbegriffen, Kapitel 4.2 "Komponenten einer GIS-Web-Lösung" stellt verschiedene Komponenten dar, Kapitel 4.3 "Technologien" liefert die entsprechenden Technologien.

Eine wichtige Bedingung soll generell berücksichtigt werden: Es ist nicht nur die Sicherheit in Bezug auf die Kommunikation zwischen Client und Server sicherzustellen. Auf Betriebssystem- und Systemmanagement-Ebene muss die Sicherheitspolitik ebenfalls eingehalten werden!

4.1 Grundanforderungen

Systeme, die über das Internet kommunizieren, müssen gewissen Grundanforderungen genügen. **Vertrauen, Integrität** und **Verfügbarkeit** sind die drei meist genannten und wichtigen, auch sicherheitsrelevante Anforderungen an die Informationen bei deren Verteilung im Internet. Für bestimmte Informationstypen in bestimmten Businessbereichen (Bank, Versicherung …) ist das Vertrauen in die Daten extrem wichtig. Kann dieser Aspekt nicht erfüllt werden, kann es weitreichende Konsequenzen haben. Unautorisierte Änderungen von Daten bewirken den Verlust der Integrität. Eine Konsequenz kann sein, dass solche Daten für den „sauberen“ Anwender nicht verfügbar sind.

Authentifizierung, Autorisierung und Zulassung gelangen zur Anwendung bei der Erstellung einer Applikation, um die Information für vertrauensvolle Kunden verfügbar zu machen.

- Authentifizierung ist der Prozess, bei dem der Anwender anhand von eindeutigen Beweisen seine Identität erbringt.
- Autorisierung ist der Prozess, bei dem bestimmt wird, welche Rechte für einen einzelnen Anwender zu implementieren sind.
- Authentifizierung und Autorisierung sind zusammen zu implementieren. Ein Anwender ist bezüglich Sicherheit und Integrität zu authentifizieren bevor er autorisierte Tasks ausführen lassen kann.

4.2 Komponenten einer GIS-Web-Lösung

Dieses Kapitel behandelt Konzeptbegriffe, Komponenten einer GIS-Web-Lösung und mögliche Technologien.

Eine Webapplikation besteht aus den Hauptkomponenten Daten-, Applikations- und Web-Server. Diese drei Teile können je nach Anforderung und technischen Möglichkeiten (Plattform) auf einem einzigen Server installiert und betrieben werden (One-Tier). Bei der Applikation wird bei GIS-Webprojekten oft von Kartenserver gesprochen. Beim Kartenserver kann weiter zwischen Applikations- und Spatialserver unterschieden werden. Anhand der Architekturbeispiele wird ersichtlich, dass unterschiedliche Grundarchitekturen miteinander gemischt und vermischt werden können.

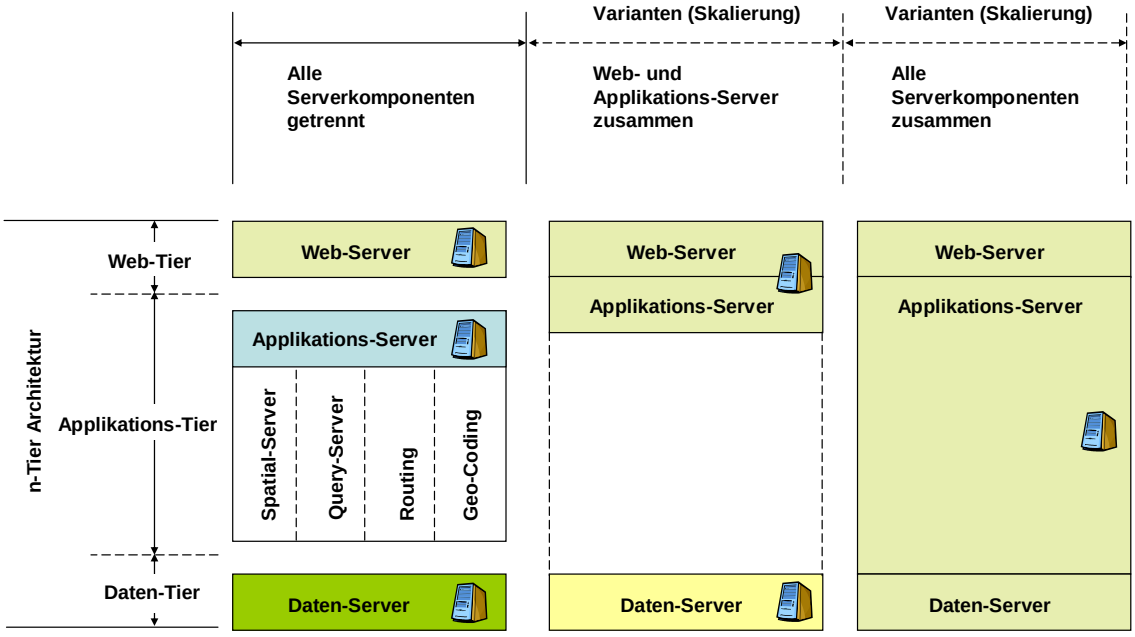


Abbildung 5: Komponenten einer GIS-Weblösung

Kommunikation

Werden die einzelnen Komponenten des GIS-Web-Servers auf separaten Servern betrieben, muss die Kommunikation zwischen Ihnen sichergestellt sein. Die Kommunikation ist abhängig von der eingesetzten Software, resp. dem Systemlieferanten. Nachfolgende Erläuterungen sollen als Beispiel betrachtet werden.

Beispiel:

Situation: Web-, Applikations- sowie Daten-Server sind physisch getrennte Einheiten.

Anfrage: Web-Client stellt via Browser eine Anfrage an der Web-Server. Die Anfrage lautet "Karte im Massstab 1:2000 mit den Daten "Amtliche Vermessung".

Prozesse:

- Web-Server nimmt die Anfrage entgegen (Annahme: Authentifizierungen etc. haben bereits stattgefunden). Die Anfrage wird für den Applikations-Server vorbereitet und in der Form eines XML-Dokuments an den Applikations-Server weitergeleitet. Das Dokument enthält die genauen Angaben der Anfrage (ev. ergänzt mit Benutzer-ID etc.).
- Der Applikations-Server prüft und verarbeitet die Anfrage. Bei fehlenden Angaben wird die Anfrage unter Umständen an den Web-Server mit der Forderung nach zusätzlichen Informationen zurückgeschickt. Bei genügend Angaben liefert der Applikations-Server die gewünschte Karte in Form einer Pixel- oder Vektordatei. Die Benachrichtigung über Ort und Name der Kartendatei erfolgt wiederum als XML-Dokument.
- Der Daten-Server dient lediglich als Datenlieferant. Die Kommunikation erfolgt nur über den Applikations-Server (z.B. Anrage via ADO und ASP-Skripten).
- Der Web-Server leitet das Resultat an den Web-Client (Browser) zurück und ergänzt die Informationen des Applikations-Server ev. mit zusätzlichen Hinweisen.

Weitere Informationen müssen bei den jeweiligen Systemlieferanten angefordert werden. Die Kommunikationsmöglichkeiten zwischen einzelnen Systemen haben sich in den letzten Jahren stark vereinfacht.

Server-Verfügbarkeit

Die Ausfallsicherheit wird auf der einen Seite geprägt von Installations- und Softwarequalität und auch von Hardwarekomponenten. Auf der anderen Seite wird die Ausfallsicherheit durch eine möglichst dichte Abschottung gegenüber dem Internet erhöht. Anforderungen an eine hohe Verfügbarkeit wie beispielsweise 7x24 (7 Tage à 24h) schlagen sich nicht unwesentlich auf den Gesamtpreis der Lösung aus (hohe Kosten). 7x24 bedeutet, dass ein IT-Dienstleister Personal und ev. Hardware rund um die Uhr bereitstellen muss.

Die Serververfügbarkeit ist abhängig von:

- Netzwerkverfügbarkeit (Verfügbarkeit der Internet-Anbindung, beispielsweise des Internet-Service-Providers ISP)
  Ist der ISP fähig, den Dienst 7x24 anzubieten? Welche Abhängigkeiten gelten für den ISP?
- Hardwareverfügbarkeit
  Wie ausfallsicher ist die Hardware? Sind die Server mit RAID 0/2/5 ausgestattet? Sind die Server gespiegelt?

- Software- bzw. Serviceverfügbarkeit
  Was passiert wenn ein Applikations-Service versagt (Absturz)? Nimmt ein zweiter Service den Platz ein? Kann das System Warnungen an Dritte weiterleiten? Kann von extern eingegriffen werden?
- Daten(-Server)verfügbarkeit
  Sind die Daten 7x24 vorhanden? Was passiert wenn die Daten nicht aktualisiert werden können? Soll in diesem Fall mit alten Daten weitergearbeitet werden?
- Personalverfügbarkeit
  Kann der IT-Dienstleister Personal innerhalb von x Stunden aufbieten?

Im Zusammenhang mit der Verfügbarkeit wird oft auch von Skalierung gesprochen. Die Skalierung von Systemen erhöht die Performance der Gesamtlösung. Der Teil Skalierung wird in diesem Artikel nicht weiter verfolgt. Skalierungsmöglichkeiten sind stark vom Applikations-Anbieter abhängig und haben einen Einfluss auf die Verfügbarkeit. Werden beispielsweise Kartendienste über sieben parallele Server skaliert um grosse Mengen von Anfragen abarbeiten zu können, muss auch die Verfügbarkeit erneut überprüft werden. Müssen alle sieben Server ausfallsicher konzipiert werden oder reicht hier ein Minimum von drei Servern parallel?

Kosten

Es gilt im Sinne eines Tipps zu beachten, dass zu Beginn einer Web-Lösung die Anforderungen an die Ausfallsicherheit nicht zu hoch gesetzt werden. Hohe Ausfallsicherheiten bringen wie erwähnt auch hohe Kosten mit sich. Oft stehen die Kosten bezüglich Ausfallsicherheit nicht mehr im Einklang mit dem Nutzen des geplanten Dienstes.

4.3 Technologien

Damit sich die Konzepte in der Praxis umsetzen lassen, werden leistungsfähige und sichere Technologien vorausgesetzt. Die gängigen Sicherheitstechnologien werden in Abbildung 6: Übersicht Technologien dargestellt und im anschliessenden Text erläutert.

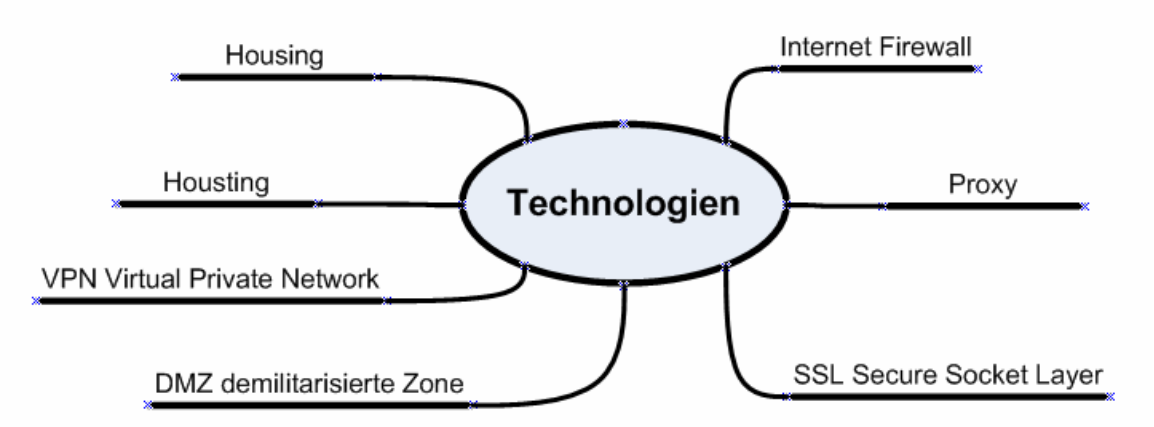


Abbildung 6: Übersicht Technologien

4.3.1 Internet Firewall

Die Firewall ist eine oder mehrere Komponenten, die den Zugriff zwischen einem geschützten Netz und dem Internet oder zwischen beliebigen anderen Netzen beschränken.

Eine Firewall ist eine Kombination von Hardware und Software Komponenten für die Untersuchung des Netzwerkverkehrs und Service-Anfragen. Nicht autorisierte Pakete oder Anfragen werden basierend auf festgelegten Regeln blockiert. Eine Internet Firewall wird an der Schnittstelle zwischen internem Netzwerk und dem Internet installiert.

Als "**Port**" wird die durch eine Zahl festgelegte Verbindung durch die Firewall bezeichnet. Ein Port dient dazu, über das Internet Protokoll (IP) übermittelte Daten den richtigen Anwendungen bzw. Diensten zuzuordnen. Man kann sich einen Port also als eine Art Buchse vorstellen, in die eine Datenverbindung hineingeht. Von Haus aus ist ein Port geschlossen, erst wenn ein Dienst diesen Port öffnet um auf diesem Anfragen entgegen zu nehmen, können über den Port Daten in den Rechner gelangen. An einen geschlossenen Port gesendete Anfragen werden vom System einfach weggeworfen und durch eine entsprechende Antwort quittiert.

4.3.2 Proxy

Ein Proxy oder forward Proxy ist ein Gateway für einen Client-Browser. Er sendet http-Anfragen von internen Clienten ins Internet. Der Proxy schützt das interne Netzwerk, indem er seine eigene IP-Adresse angibt. Diese deckt seine Clienten. Der fremde, aussenstehende http-(Web)Server sieht als Absender nicht die Adresse des internen Clienten, sondern diejenige des Proxy.

Ein reverse Proxy funktioniert zugunsten des http-Servers und nicht zugunsten der Clienten. Er stellt für aussenstehende Anfragen seine Adresse zur Verfügung. Die Internet Firewall stellt sicher, dass nur der reverse Proxy Zu-

gang zum geschützten http-Server erhält. Aussenstehende Clienten erkennen den reverse Proxy als aktuellen http-Server.

4.3.3 SSL

SSL ist ein von Netscape entwickeltes Protokoll, das auf symmetrischen und asymmetrischen Algorithmen basiert, um eine gesicherte Transaktion von zwei Endpunkten zu gewährleisten. Das SSL-Protokoll schafft unter drei Gesichtspunkten sichere Verbindungen:

1. Die Verbindung ist im besten Sinne privat, weil ihr Inhalt nur verschlüsselt über das Netz geht.

2. Die Identität des Servers steht fest.

3. Wirkungsvolle Algorithmen prüfen, ob die Daten vollständig und unverändert ihren jeweiligen Empfänger erreichen.

Vor fast 30 Jahren wurde TCP/IP erfunden. Dabei war das Ziel, eine ausfallsichere und stabile Verbindung mit hoher Betriebssicherheit zu schaffen. Die Sicherheit und Authenzität der übermittelten Daten spielte eine untergeordnete Rolle. Mit TCP/IP war der Wunsch nach sicheren Verbindungen im Sinne von Datensicherheit nicht zu verwirklichen. Die Firma Netscape löste das Problem auf folgende elegante Weise: Die Entwickler erweiterten TCP/IP um zwei weitere Schichten (SSL Record- und SSL Handshake-Protocol).

4.3.4 DMZ

Zusätzlicher bzw. n-zusätzliche Layer zwischen externem Netzwerk (Internet) und Intranet. Die Realisierung erfolgt durch die Zwischenschaltung von Hard- und Software in Kombination mit einem eigenen Netzwerk (eigene Adress-Bereiche). Eine sogenannte demilitarisierte Zone (DMZ) ist nicht zwingend auf einen Layer beschränkt. Der Begriff Zone kann demnach weitgehend als ein weiteres Massnahmen-Paket zur Sicherung der Server resp. Daten betrachtet werden.

Funktionsweise: Die DMZ unterteilt die Hardware, Software und die eingesetzten Protokolle (!) durch den Einschub einer weiteren Firewall. Nachfolgende Beispiele veranschaulichen eine Auswahl der Möglichkeiten.

Alle GIS-Web-Komponenten in der DMZ

- Anordnung der Komponenten:
  Web-Server, Applikations-Server und Daten-Server ausserhalb der Intranet Firewall in der DMZ.
- Datensicht:
  Die Datenbearbeitung erfolgt im Intranet. Für die Publizierung wird die Erstellung einer Datenkopie (Duplizierung, Replikation) notwendig.
- Kommunikation:
  Klienten kommunizieren i.a. durch Port 80 mit dem Web-Server.

Kein Öffnen weiterer Ports notwendig, da alle Komponenten an einem Ort.

- Wartung:
  Wartung der Services soll durch den offenen Port gewährleistet sein.
- Fazit: einfache, populäre Architektur.

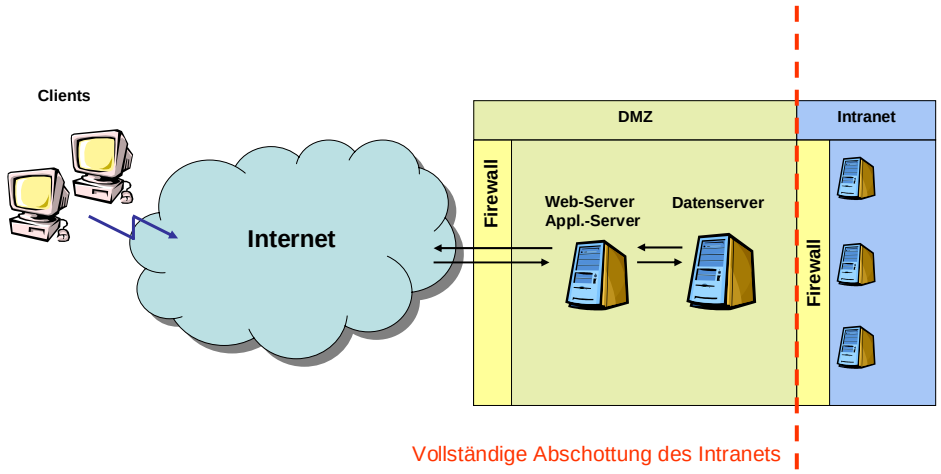


Abbildung 7: Alle GIS-Komponenten in der DMZ

Daten-Server ausserhalb DMZ

- Anordnung der Komponenten:
  Web-Server und Applikations-Server ausserhalb der Intranet Firewall in der DMZ.
- Datensicht:
  Die Datenbearbeitung erfolgt im Intranet.
  Die Webapplikation greift durch die sichere Firewall auf den internen (GIS-)Daten-Server und durch einen Port mit limitiertem Zugriff auf den Daten-Server zu.
- Kommunikation:
  Klienten kommunizieren i.a. durch Port 80 mit dem Web-Server.
  Firewall verbietet anderen Quellen als dem Applikations-Server den Zugang zum Intranet.

- Wartung:
  Wartung der Services soll durch den offenen Port gewährleistet sein. Datenduplizierung entfällt.
- Fazit:
  Sicherheitsgewährleistung bei Zugriff durch Kartenservice und DBMS. Ausfallsicherheit des Daten-Servers durch Firewall und Intranet beeinträchtigt.

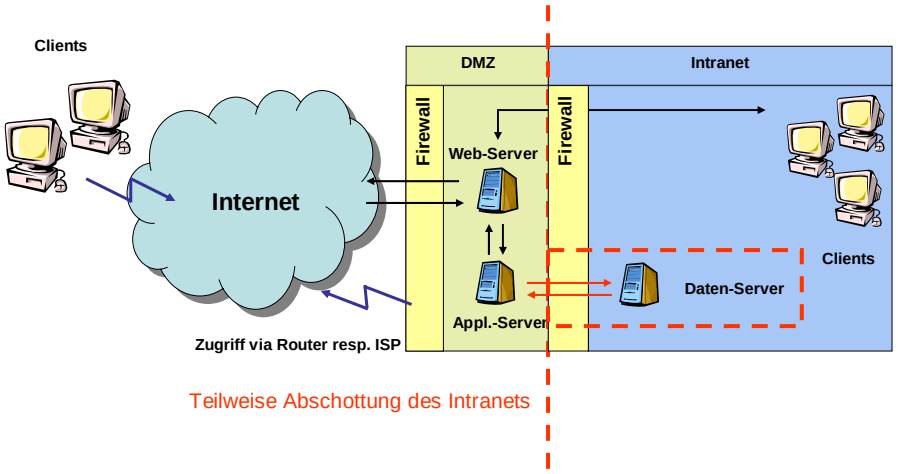


Abbildung 8: Daten-Server ausserhalb der DMZ

Daten- und Applikationsserver ausserhalb DMZ

- Web-Server in der DMZ. Applikations-Server und (GIS-)Daten-Server im Intranet.
- Klienten kommunizieren durch Port 80 der Internet Firewall mit dem Web-Server.
- Web-Server und Applikations-Server kommunizieren durch einen Port der Intranet Firewall.
- Die Output-Files werden (temporär) auf dem Web-Server geschrieben, welche für den Spatial-Server (one-way) geshared werden.

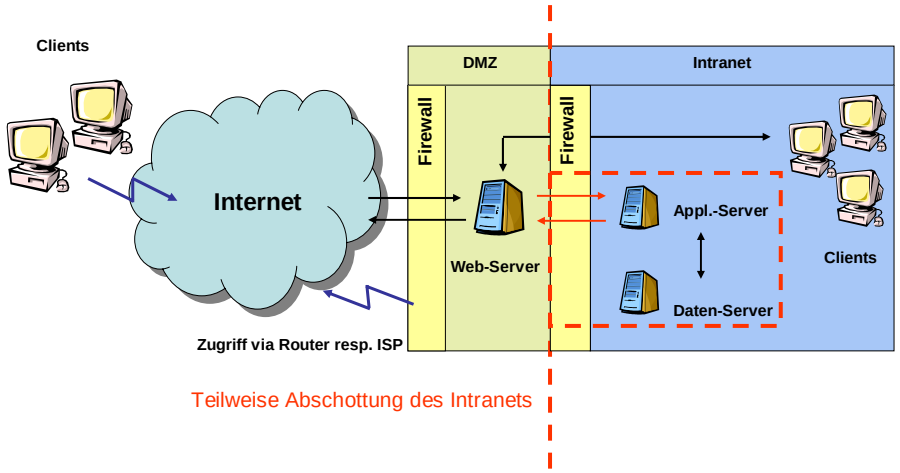


Abbildung 9: Daten- und Applikationsserver ausserhalb DMZ

Gesteigerte Variante: Proxy-Server in der DMZ

- Sicherheit des privaten Netzwerks durch einen Proxy-Server.
- Vollständige Web-Konfiguration im privaten Netzwerk.
- Client Browser kommunizieren durch Port 80 der Firewall mit Proxy-Server.
- Proxy-Server kommuniziert durch Port 80 der Firewall mit Web-Server im internen Netzwerk.

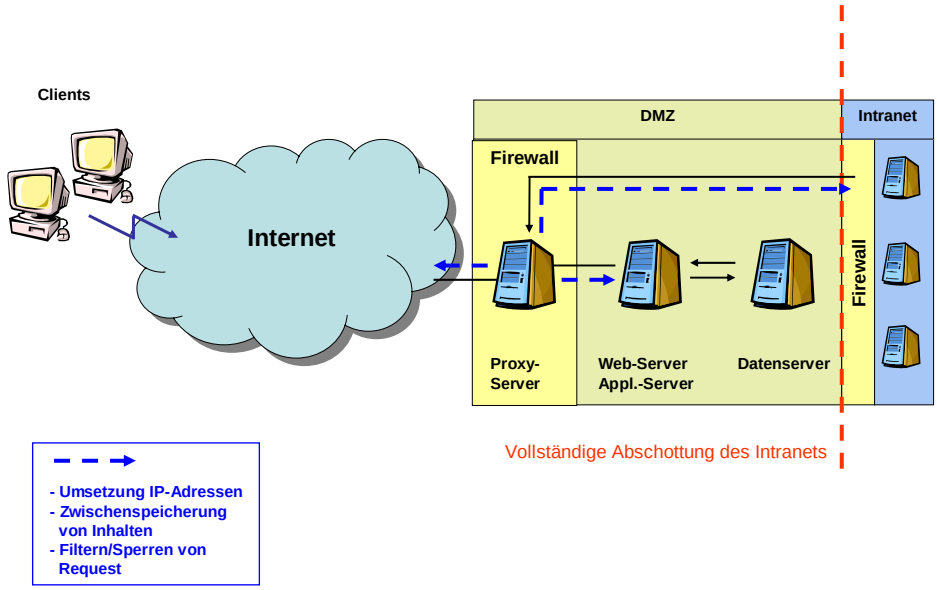


Abbildung 10: Proxy-Server in der DMZ

Weitere mögliche Varianten

Die Komponenten des Applikations-Servers werden weiter auf verschiedene Server verteilt. So kann zum Beispiel der Spatial-Server und der Daten-Server in Secure Network betrieben werden. Dies ist machbar, aber meist nicht sinnvoll.

Eine multiple (bzw. hybride) Web-Server Konfiguration wird anhand von 2 Fällen skizziert:

- Die Verbreitung im Intranet und Internet erfolgt durch separate Web-Server. Der Web-Server für das Internet steht i.a. in der DMZ und kommuniziert durch die Intranet Firewall mit dem Applikationsserver.
- Mehrere Applikations-Server sind bei sehr grosser Anzahl von Anfragen (Peak) notwendig.

4.3.5 VPN

Durch den Einsatz von VPN-Security-Lösungen (Virtual Private Network) werden Gefahren abgewehrt. Die Kommunikation durch das Internet erfolgt nur über authentisierte und vollständig verschlüsselte Kanäle (sogenannte Tunnel). Die Daten werden so wirkungsvoll geschützt und ihre Übertragung kontinuierlich überwacht. Die technische Basis für VPN bildet das Protokoll IPsec. IPsec beinhaltet vier wichtige Sicherheitsfunktionen:

- Verschlüsselung - als Schutz gegen unbefugtes Mitlesen
- Authentisierung der Nachricht - zum Beweis der Unverfälschtheit einer Nachricht (Paketintegrität)
- Authentisierung des Absenders - zur unzweifelhaften Zuordnung eines Senders/ Empfängers (Paketauthentizität)
- Verwaltung von Schlüsseln

Beispiel: Zwischen der Zentrale und der Niederlassung besteht eine permanente Internet-Verbindung für den sofortigen Zugriff auf gemeinsame Ressourcen. Mobile Mitarbeiter (z.B. Außendienst, Teleworker oder leitende Angestellte) greifen bei Bedarf von außerhalb auf das Netz der Zentrale oder der Niederlassung zu. Durch starke Authentisierungs- und Autorisierungsmechanismen ist der Zugriff nur für die jeweils zugelassenen Benutzer möglich. Weil der gesamte Datenverkehr innerhalb des Internets verschlüsselt wird, bleiben die übertragenen Daten vertraulich und geschützt. Jeder Mitarbeiter kann auf alle für ihn relevanten Daten zugreifen. Aber gleichzeitig werden alle unbefugten oder unkontrollierten Zugriffsversuche abgewehrt.

4.3.6 Hosten

Bei der Betreibung des Web-Dienstes könnten alle Hard- und Software sowie Service-Leistungen im Haus erbracht werden. Oft will der Betreiber, dass gewisse Leistungen von Extern erbracht werden. Ein Outsourcing Partner ist der Internet Service Provider (ISP). Er bietet die Möglichkeiten von Hosting und von Housing.

Hosting

Internet Service Provider (ISP) stellen Hard- und Software zur Verfügung, um einen Web-Dienst zu betreiben (z.B. Firmenhomepage). ISP ist für die Sicherheit verantwortlich.

Housing

Internet Service Provider (ISP) stellt Platz für Hardware zur Verfügung. Der Kunde kann den Server selber warten. Der Kunde hat in der Regel ausschliesslich einen Netzwerkanschluss zur Verfügung. Sicherheit ist Aufgabe des Kunden. Housing, bei welchem die Sicherheit (Firewall etc.) durch ISP abgedeckt wird, ist heute eher selten und zudem teuer.

Eine gemischte Variante, bei der das Monitoring und das Sicherheitsmanagement outsourced werden, bietet folgende Vorteile:

- IT-Sicherheitsheits-Spezialwissen wird eingekauft
- Die IT-Komponenten (HW, SW) sind eigen und im Haus.
- Das Monitoring und Management der Sicherheitsgeräte (Firewall) erfolgt vom Spezialisten von extern.

- Ein solches Outsourcing wird heute oft nicht verfolgt, weil dem externen Dienstleister kein Teilzugang zur firmeneigenen Infrastruktur aus Sicherheitsüberlegungen ermöglicht wird.

4.3.7 Technologie-Einsatz pro Grundanforderung

Als Beispiel für die Erfüllung einer Grundanforderung wird mit nachfolgender Matrix pro Grundanforderung je eine Technologie aufgeführt. Die Liste ist beispielhaft und nicht abschliessend.

Grundanforderung	Technologie
Vertrauen	SSL (Verschlüsselung, Kryptographie)
Integrität	Digitale Unterschrift
Verfügbarkeit	Server-Spiegelung (Raid, etc.)
Authentifizierung	Passwort, Secur-ID, Kartenleser
Autorisierung	Security-Policy (Autorisierungs-Datenbank)
Zulassung	Firewall

5 Szenarien, Anwendungsbeispiele und Konfigurationsbeispiele aus dem GIS-Bereich

Folgende Szenarien, Anwendungs- und Konfigurationsbeispiele zeigen Kombinationen verschiedener Architekturen und Zugriffstechniken. Die Auflistung der Beispiele ist nicht abschliessend.

Zudem gilt zur Vereinfachung folgende Annahme: Web- und Applikations-Server werden in einer Hardware-Komponente zusammengefasst. Einzig der Daten-Server wird von den anderen Komponenten losgelöst dargestellt. Der Grund für die Trennung des Daten-Servers liegt in den vielfältigen Möglichkeiten der Datenbereitstellung.

Bei den Daten auf dem Daten-Server kann es sich um die Produktionsdaten oder aber um eine Replikation (Sekundär-Datenbank) handeln. Die Konfigurationsbeispiele berücksichtigen diese beiden Möglichkeiten. Die Trennung ist demnach graphischer Natur.

Die dargestellten Szenarien und ihre Varianten unterscheiden sich wie folgt:

- Szenario 1: Datenherr betreibt Daten-Server selber
  - Variante A: nur interner Datenzugriff (Intranet)
  - Variante B: interner und externer Datenzugriff (Intranet/Internet)
- Szenario 2: Datenprovider betreibt Daten-Server für Datenherrn
  - Variante A: Daten-Server steht beim Datenprovider
  - Variante B: Daten-Server steht extern beim Internet Service Provider
- Szenario 3: Mehrere Datenherren betreiben Daten-Server gemeinsam

5.1 Szenario 1: Datenherr betreibt Daten-Server selber

5.1.1 Variante A: nur interner Datenzugriff (Intranet)

Merkmale:

- Daten liegen beim Datenherr
- Zusätzliche Daten (Naturschutz, etc.) werden eingekauft und müssen integriert werden
- Keine speziellen Ansprüche an IT-Sicherheit, da nur Intranetlösung (kann via normale IT-Security gelöst werden)
- Datensichtung mit/ohne Passwortschutz

Anwendungsbeispiel: Kantonales GIS-Zentrum

Ein kantonales GIS-Zentrum verwaltet alle Geodaten des ganzen Kantons auf einem eigenen Server. Zurzeit greifen nur kantonale Ämter (also Intranet) auf die Daten zu. Externen Nutzern sind die Daten nicht online verfügbar.

Daten verschiedener Ämter müssen integriert werden. Eigene Daten werden nur in geringem Masse erstellt.

Konfigurationsbeispiel:

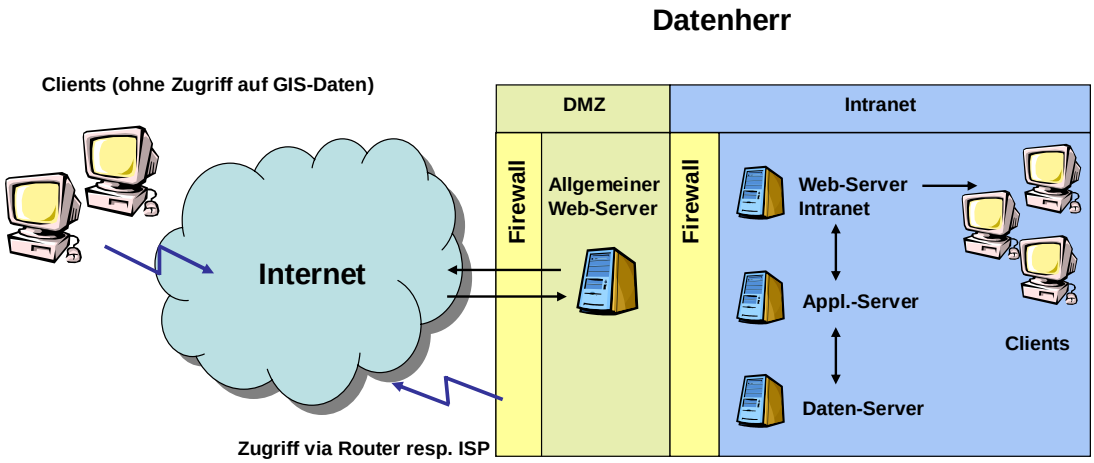


Abbildung 11: nur interner Datenzugriff (Intranet)

Bemerkung:

- Lesezugriffe nur innerhalb des Intranets

5.1.2 Variante B: interner und externer Datenzugriff (Intranet/Internet)

Merkmale:

- Daten liegen beim Datenherr
- Zusätzliche Daten (Naturschutz etc.) werden eingekauft und müssen integriert werden
- Ansprüche an IT-Sicherheit hoch, da durch Internet-Lösung einerseits die Daten einem breiten Publikum zur Verfügung gestellt werden (ev. nur Teile der Daten) und andererseits die allgemeine IT-Security überdacht werden muss (falls der Server beim Datenherr steht) → Hackerangriffe etc.

- Datensichtung mit/ohne Passwortschutz, falls nur Teile der Öffentlichkeit zugänglich sind
- Datenhaltung ist wichtig. Soll für den Internetzugriff eine redundante Datenhaltung eingeführt werden?
  Bemerkung: Dies wird in der Regel bereits für Szenario1 berücksichtigt

Anwendungsbeispiel: Vertriebsfirma für Konzerttickets

Die Firma arbeitet nur mit wohl definierten Kunden zusammen, sie vertreibt Wertpapiere übers Internet. Die Abgabe der Tickets ist kostenpflichtig (sowohl das Ticket selber als auch der Bezug eines solchen). Die Firma verfügt über eine eigene Infrastruktur (SW und HW).

Konfigurationsbeispiel ohne Verschlüsselung:

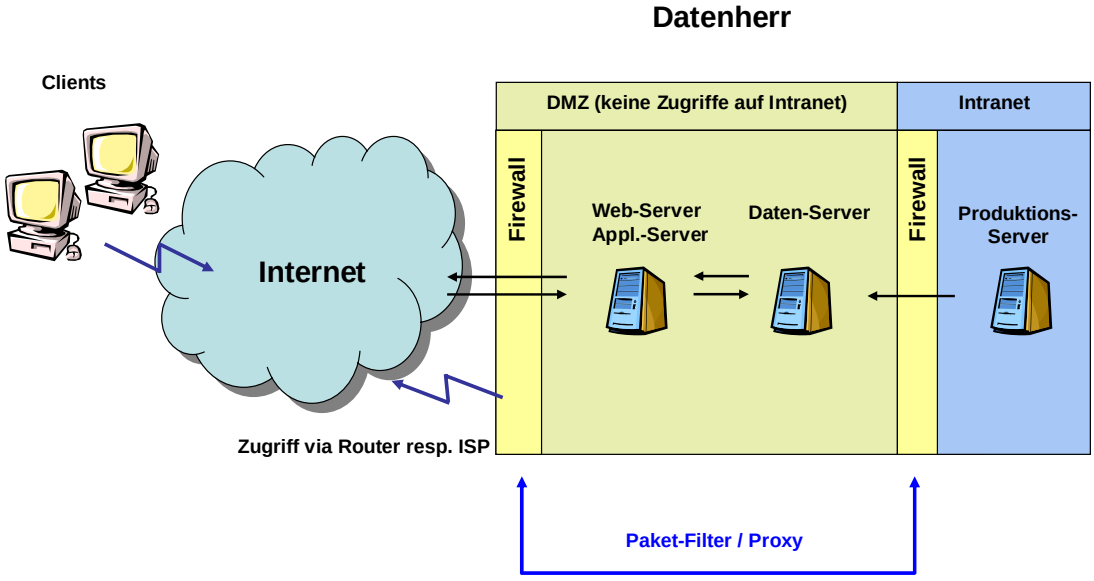


Abbildung 12: interner und externer Datenzugriff

Bemerkungen:

- Lesezugriffe auf Internet ausgedehnt
- Zugriff ohne Passwortschutz (öffentlich zugängliche Daten)
- Daten werden repliziert

Konfigurationsbeispiel mit Verschlüsselung:

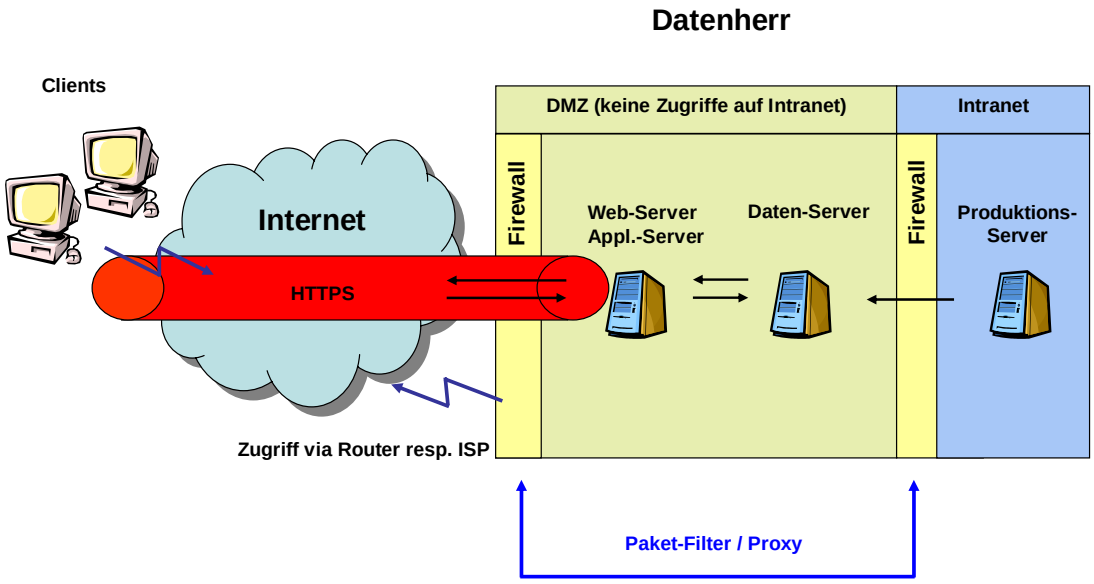


Abbildung 13: interner und externer Datenzugriff mit Verschlüsselung

Bemerkungen:

- Lesezugriffe auf Internet ausgedehnt
- Zugriff mit Passwortschutz und Verschlüsselung (Datenzugriff auf bestimmte Benutzergruppen eingeschränkt)
- Daten werden repliziert

5.2 Szenario 2: Datenprovider betreibt Daten-Server für Datenherrn

5.2.1 Variante A: Server steht bei Datenprovider

Merkmale:

- Kunde greift via Standleitung/Breitband etc. auf die Daten zu
- Datensichtung mit/ohne Passwortschutz, falls nur Teile der Öffentlichkeit zugänglich sind
- Daten liegen in DMZ, Intranet
- Performance ist abhängig von Verbindung Datenprovider – Web-Provider (Hosting) - Kunde

Anwendungsbeispiel: grosses Geometerbüro

Das Geometerbüro ist genügend gross und verfügt über eine geeignete Infrastruktur, um die Daten auf einem eigenen Server zu halten.

Geometer will seine AV-Daten der Öffentlichkeit kontrolliert zur Verfügung stellen. Das heisst, je nach „Rolle“ des Benutzers kann er nur Bilder runterladen oder er hat Zugang zu Vektordaten oder kann diese sogar bearbeiten. Der Bezug der Daten ist kostenpflichtig.

Konfigurationsbeispiel ohne Verschlüsselung:

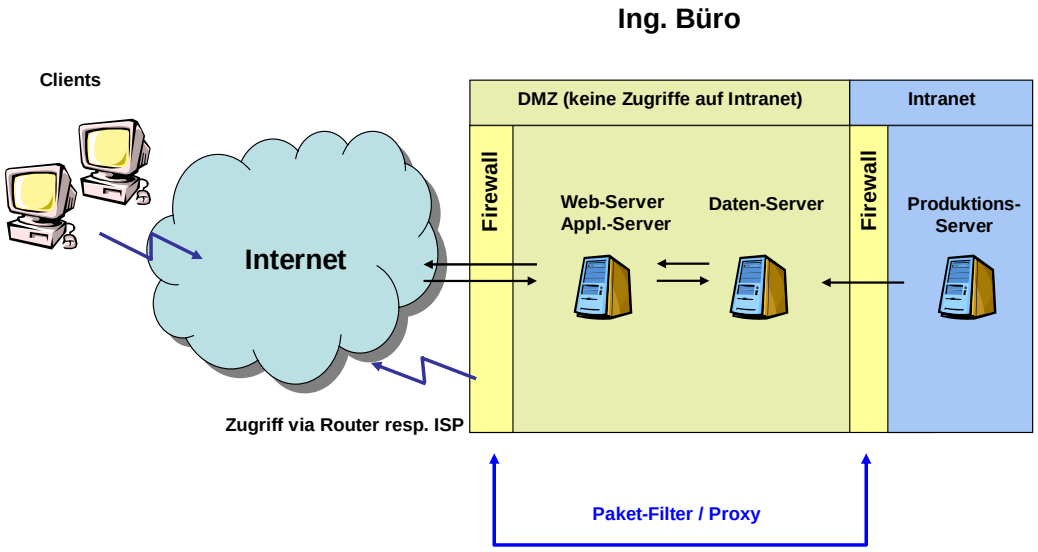


Abbildung 14: Konfigurationsbeispiel ohne Verschlüsselung

Bemerkungen:

- Nur Lesezugriff benötigt, daher werden Produktionsdaten in DMZ repliziert
- Durch die heutigen Breitbandanschlüsse wie ADSL oder Kabelfernsehen (z.B. "Cablecom", GGA-Maur) kann es sich der Datenprovider heute technisch und finanziell leisten, den Web-Auftritt selbst zu organisieren. Dafür wird im Minimum folgendes vorausgesetzt: Breitbandanschluss, Router, Hardware und Betriebssystem (Internet-Service wie IIS von Microsoft), DNS-Einträge beim Provider (damit die Namensauflösung funktioniert), Sicherheitsrelevante Einrichtungen (Firewall, Virenschutz, etc.)
- Je nach Anforderungs- und Automatisierungsgrad wird die Trennung in Produktions- und Daten-Server- Betrieb komplexer. Die Komplexität ist zudem von der Gesamtarchitektur des Netzwerks des Datenproviders abhängig.

Konfigurationsbeispiel mit Verschlüsselung:

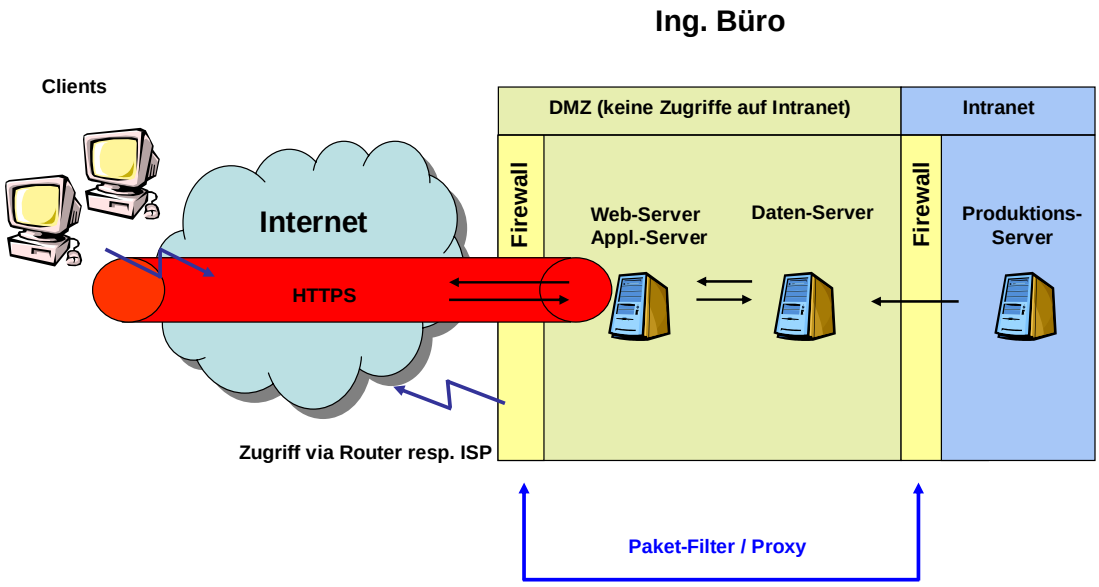


Abbildung 15: Konfigurationsbeispiel mit Verschlüsselung

Bemerkungen:

- Nur Lesezugriff benötigt, daher werden Produktionsdaten in DMZ repliziert
- Zugriff der Clients durch verschlüsselte Verbindung (SSL → HTTPS oder VPN)

5.2.2 Variante B: Server steht extern bei Internet Service Provider (ISP)

Merkmale:

- Kunde greift auf die Daten via Internet zu
- Datensichtung mit/ohne Passwortschutz, falls nur Teile der Öffentlichkeit zugänglich sind
- Daten bzw. Server sind in der Regel durch den Web-Provider nicht speziell geschützt (wer ist für die Sicherheit verantwortlich?). Geschütztes "Housing" ist sehr teuer (siehe Begriffe Kapitel 3).
- Performance abhängig von Verbindung Datenprovider – Web-Provider und Web-Provider – Kunde
- Daten müssen "periodisch" via upload aktualisiert werden (wie oft, wie schnell?)

Anwendungsbeispiel: kleines Geometerbüro

Das Geometerbüro ist ein 3-Mann-Betrieb und verfügt nicht über die geeignete Infrastruktur.

Geometer will seine AV-Daten der Öffentlichkeit kontrolliert zur Verfügung stellen. Das heisst, je nach „Rolle“ des Benutzers kann er nur Bilder runterladen oder er hat Zugang zu Vektordaten oder kann diese sogar bearbeiten. Der Bezug der Daten ist kostenpflichtig.

Konfigurationsbeispiel ohne Verschlüsselung:

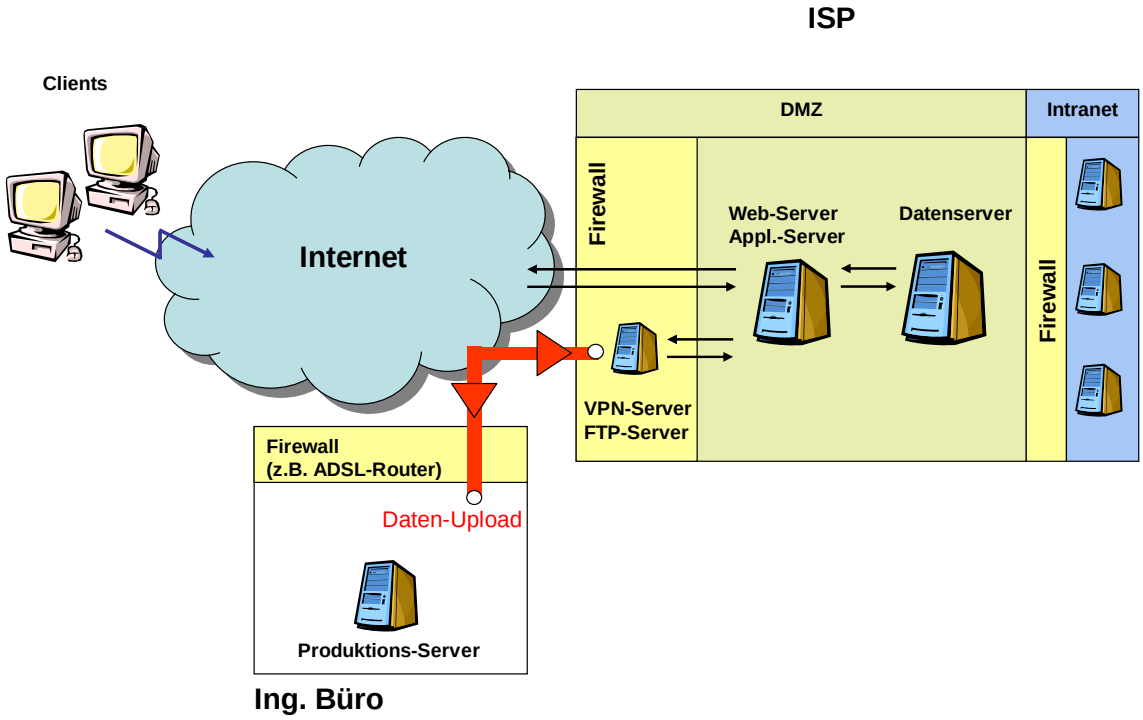


Abbildung 16: Konfigurationsbeispiel ohne Verschlüsselung

Bemerkungen:

- Anstelle von VPN-Verbindung kann auch FTP-Upload gewählt werden.
- Bei der aufgezeigten Variante wird davon ausgegangen, dass keine Schreibrechte auf die Daten gefordert sind.
- Diese Konfiguration trägt der Situation Rechnung, dass der Produktionsbetrieb (im Beispiel das Ing. Büro) über keine entsprechende Server-Infrastruktur verfügt.
- Varianten: Der ISP stellt entweder Hardware und Betriebssystem (Hosting) oder ausschliesslich den Internet-Anschluss (Housing) zur Ver-

fügung. Beides hat Vor- und Nachteile. In den meisten Fällen ist bei der Variante Housing der Auftraggeber für die Sicherheit des Web-Servers zuständig. Wird die Variante Hosting gewählt, sind oft die Administrationsfreiheiten eingeschränkt (→ keine Möglichkeit, Software selbständig zu Installieren/Warten).

Konfigurationsbeispiel mit Verschlüsselung:

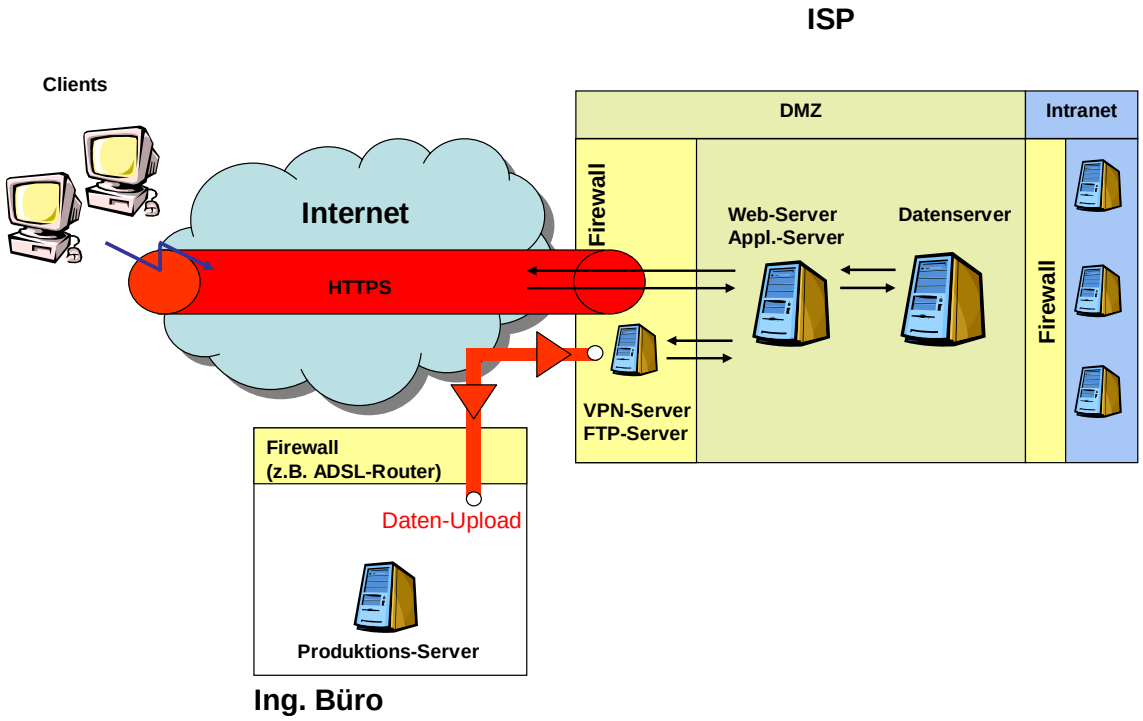


Abbildung 17: Konfigurationsbeispiel mit Verschlüsselung

Bemerkung:

- Datenzugriff verschlüsselt

5.3 Szenario 3: Mehrere Datenherren betreiben gemeinsamen Daten-Server

Merkmale:

- Kunde greift auf die Daten via Internet zu
- Datenzugriff teilweise via Passwortschutz

- Schutzmöglichkeiten via VPN-Server oder verschlüsselt (HTTPS). Einsatz eines VPN-Servers eher für eine kleine und bestimmte Anzahl von Anwendern (ca. 50). Sonst sollte HTTPS verwendet werden.
- Performance abhängig von Verbindung – Provider – Kunde
- Teile der Daten müssen "periodisch" via upload aktualisiert werden (wie oft, wie schnell, nach welchen Kriterien?)
- Verschiedene Formate erschweren den Datenupload (→ INTERLIS als mögliche Lösung!)
- Verrechnung der Datenzugriffe?
- Erweiterung der Funktionalität: Datenzugriff teilweise mit Schreibrechten

Anwendungsbeispiel 1: Umweltschutzamt

Umweltschutzamt hat Monitoring-Daten und will diese jedermann zugänglich machen. Die Daten werden nur intern bearbeitet und können gratis bezogen werden (übers Netz). Das Amt kann den kantonalen Daten-Server und Internetauftritt nutzen.

Anwendungsbeispiel 2: KOGIS Metadatenkatalog

Die KOGIS ist daran, einen schweizweiten Metadatenkatalog aufzubauen. Sie stellt dafür auch die Software (geocat.ch) zur Verfügung und bei Bedarf die Hardware (Daten-Server, Web-Server). Es gibt drei Arten der Benutzer:

- Pflege der Metadaten auf dem KOGIS-Server
- Pflege der Metadaten auf einem eigenen Server, der online am KOGIS-Server hängt
- Pflege der Metadaten auf einem eigenen Server mit periodischem „Batch“-Update auf den KOGIS-Server

Konfigurationsbeispiel ohne VPN-Server:

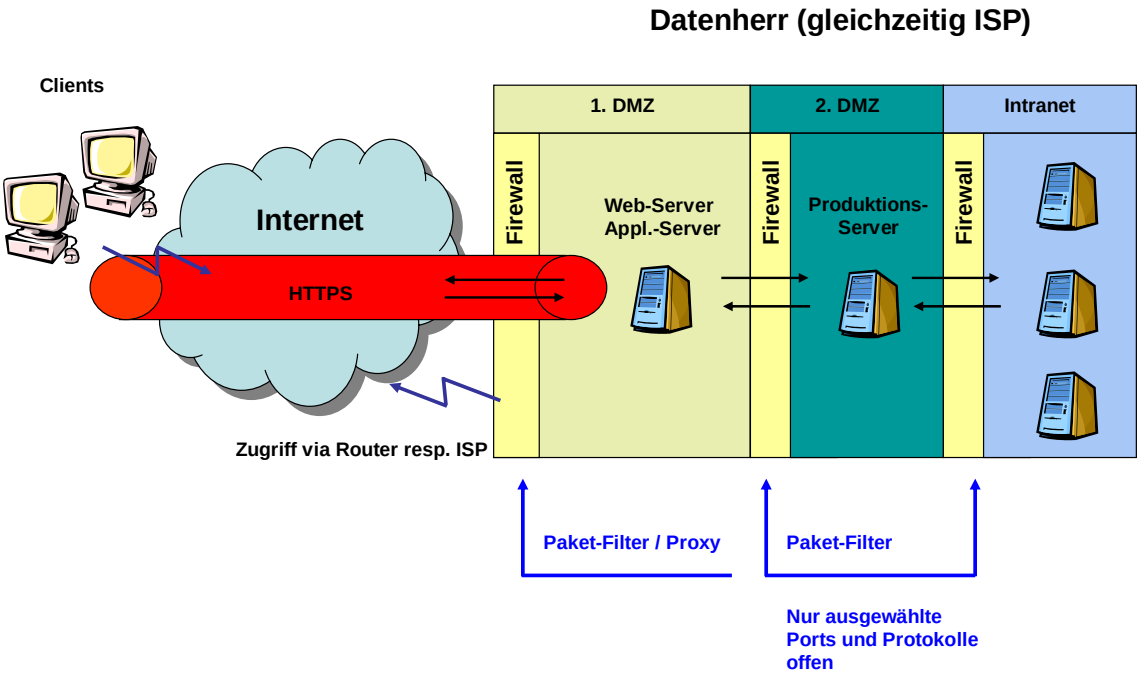


Abbildung 18: Konfigurationsbeispiel ohne VPN-Server:

Bemerkungen:

- Lese- und Schreibzugriffe
- Zugriff der Clients durch verschlüsselte Verbindung (SSL → HTTPS)
- Kommt zum Einsatz bei grosser Anzahl an Clients

Konfigurationsbeispiel mit VPN-Server:

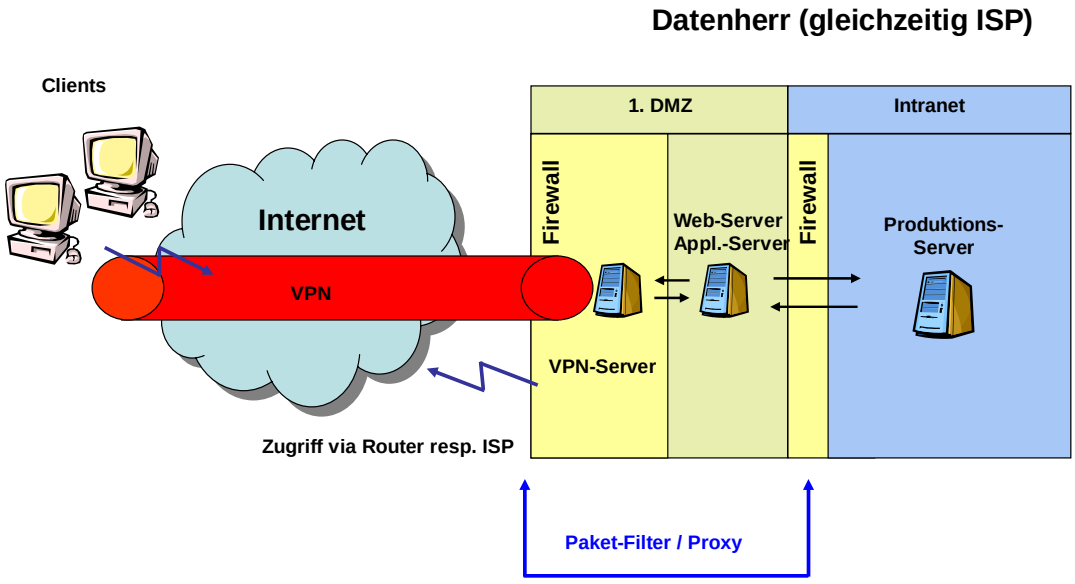


Abbildung 19: Konfigurationsbeispiel mit VPN-Server

Bemerkungen:

- Lese- und Schreibzugriffe
- Zugriff der Clients durch verschlüsselte Verbindung (VPN-Server)
- Kommt zum Einsatz bei grosser Anzahl an Clients

5.4 Weitere Aspekte

Für die Realisierung der aufgezeigten Architektur-Varianten müssen gewisse Rahmenbedingungen abgeklärt werden. Zudem sind weitere Konfigurationen unbedingt zu berücksichtigen.

Eine den Sicherheitsanforderungen entsprechende Architektur ist immer eine Kombination verschiedener Massnahmen! Wie detailliert der Leser des Artikels über Konfigurationsdetails in Kenntnis sein muss, ist immer individuell. Der Detaillierungsgrad der Konfigurationsangaben ist deshalb nicht abschliessend im Sinne einer "bullet proofed"-Auflistung zu verstehen. Zudem sollen die organisatorischen Massnahmen wie Rekrutierung und Ausbildung der Mitarbeiter nicht vergessen werden.

Rahmenbedingungen, welche auf die Realisierung einen Einfluss haben:

- Wer sind die potentiellen Ansprechpartner für GIS-Web-Server Lösungen von Gemeinden und Ingenieurbüro?
- Was sind Aufgaben bei einer GIS-Web-Server Lösung, die ein Mitarbeiter der Gemeinde bzw. Ing. Büro übernehmen kann?
- Welche Vorkenntnisse sollte der Mitarbeiter mitbringen?
- Was sind mögliche Argumente, dass ein Büro den GIS-Web-Server selbst betreibt? Oder eben nicht selbst betreibt?

Allgemeine Systemkonfigurationen

- Verschiedene Logins für verschiedene Netzwerkbereiche
- Nur betriebsrelevante Software installieren
- Verschiedene Netzwerkkarten
- Nur wichtigste (notwendige) Ports und Protokolle zulassen
- Verwenden von verschiedenen Subnets (benötigt Router-Konfiguration)
- Firewall-Konfigurationen anwenden: Proxy-Server und Paket-Filterung
- Virenschutzsoftware!
- Virenpattern sobald verfügbar updaten!
- Betriebssystem- und Applikations-Patches sobald verfügbar updaten!
- DMZ: Eventuell verschiedene DMZ für unterschiedliche Services (Email und Web durch verschiedene Firewalls bzw. DMZ trennen)

Zusätzliche System- und Applikationskonfigurationen:

- Authentifikation durch ID und Streichlisten-Nummer (ev. zusätzlich in Verbindung mit Kartenleser noch sicherer)
- Digitale Unterschrift
- Verschlüsselung (128Kbit-Verschlüsselung)

Server-Verfügbarkeit

Die Ausfallsicherheit wird auf der einen Seite geprägt von Installations- und Softwarequalität, aber auch von den Hardwarekomponenten. Auf der anderen Seite wird die Ausfallsicherheit durch eine möglichst dichte Abschottung gegenüber dem Internet erhöht.

Kommunikation

Werden die einzelnen Komponenten des GIS-Web-Server auf separaten Servern betrieben, muss die Kommunikation zwischen ihnen sichergestellt sein.

Können die einzelnen Serverkomponenten miteinander kommunizieren, können auch Daten ausgetauscht werden. Lesende und schreibende Zugriffe auf Daten sind abhängig von der Applikation. Ein Datenaustausch erfolgt beispielsweise durch XML oder JPG. Weitere Informationen liefert der Systemlieferant. Je nach Datensensibilität müssen die Daten verschlüsselt übertragen werden.

6 Anhang

6.1 Checklisten Sicherheit bei Web-Lösungen

6.1.1 Bestandesaufnahme

- Welche Daten sollen veröffentlicht werden?
- Wie heikel sind diese Daten?
- Wie sind die Daten heute gesichert? Wo sind sie gespeichert/ archiviert?
- Wie oft werden Sicherheitskopien der Daten angefertigt?
- Welche Aussagen macht das Gesetz zu diesen Daten?
- Wie beurteilt der Datenschutzbeauftragte eine Veröffentlichung der Daten?
- Was wollen Sie anbieten? B2B (Business to Business) oder B2C (Business to Customer)?
- Wie beurteilen Sie den Kenntnisstand Ihrer MitarbeiterInnen betr. Sicherheit und Risiko im Internet?
- Gibt es in Ihrer Firma bereits ein Sicherheitskonzept? Wenn ja, wird es eingehalten?

6.1.2 Bedrohungsanalyse

- Welche Sicherheitsvorkehrungen bestehen heute im System?
- Wie einfach ist das System „knackbar“?
- Wie ist der Zutritt zu den Daten geregelt (Autorisierung)?
- Wo werden die Daten abgespeichert?
- Wer hat Zugriff auf die Daten? Und wer soll in Zukunft Zugriff haben?
- Bestehen Datenredundanzen?
- Welche Systemarchitektur ist vorhanden?
- Gibt es „offene“ Leitungen im System?
- Wer hat ein Interesse daran, diese Daten zu „klauen“ oder zu „haken“?

6.1.3 Eintretenswahrscheinlichkeit

- Wie gross ist das Risiko, dass jemand die Daten „klauen“ will?
- Wie gross ist das Risiko, dass das System geknackt wird?
- Wie gross ist das Risiko, dass Daten von intern gehakt werden (absichtlich oder unabsichtlich)?

- Wie gross ist das Risiko, dass Daten von extern gehakt werden (absichtlich oder unabsichtlich)?

6.1.4 Schadenshöhe

- Was würde passieren, wenn jemand die Daten „hakt“? Szenarien
- Wie gross ist der Schaden an den Daten?
- Existieren Pläne, wie die Daten wiederhergestellt werden bei einem Datenverlust?
- Dauer/ Kosten zur Wiederherstellung der Daten?
- Wie gross ist der Schaden am System?
- Wie gross ist der Arbeitsausfall?

6.1.5 Netzwerk

a) Router

- Sind die neusten Patches und Updates installiert?
- Wurden nicht verwendete Ports gesperrt?
- Sind die administrativen Schnittstellen gesichert?
- Wurden nicht verwendete Dienste deaktiviert?
- Welche Richtlinien bestehen bei der Verwendung von Passwörtern?

b) Firewall

- Sind die neusten Patches und Updates installiert?
- Wurden Filter zur Abwehr unerwünschter Inhalte installiert?
- Wurden nicht verwendete Ports und Protokolle gesperrt?
- Wurde IPsec für die verschlüsselte Kommunikation installiert?

6.1.6 Web-Server

- Sind die neusten Patches und Updates installiert?
- Wurden nicht verwendete Dienste (speziell FTP,SMTP, NNTP) deaktiviert?
- Laufen die Dienste unter Konten mit minimal erforderlichen Berechtigungen?
- Ist der Telnet-Dienst ist deaktiviert?
- Ist NetBIOS ist deaktiviert?
- Wurden nicht benötigte Dienst- und Benutzerkonten entfernt?
- Ist der Administratoren-Zugriff ist streng gesichert?

- Ist der Web-Server ist für die „normalen“ Anwender nicht sichtbar?
- Wurden unnötige Datei- und Verzeichnisfreigaben entfernt?
- Besteht auf den verbleibenden Freigaben ein restriktiver Zugriff?
- Wurden nicht verwendete administrative Freigaben entfernt?
- Werden fehlgeschlagene Anmeldungen überwacht?
- Werden die Log-Dateien regelmässig analysiert und archiviert?
- Wurden potentiell gefährliche virtuelle Verzeichnisse (z.B. IISSamples, IISAdmin, IISHelp, Scripts beim IIS) entfernt?
- Wurden Include-Verzeichnissen die Lese-Berechtigung des Web-Servers entzogen?
- Ist der Schreib-Zugriff auf Verzeichnissen erlaubt, die die Inhaltsüberwachung unterstützen?
- Ist die entfernte Administration des Servers gesichert (Verschlüsselung, kleines Sitzungs-Timeout)?

6.1.7 Datenbankserver

- Wurden nicht benötigte Tools und Dokumentationen (Upgrade, Handbücher, Entwicklungswerkzeuge, etc.) entfernt?
- Besteht eine strenge Passwortregelung für die administrativen Konten der Datenbank-Software?
- Wurden die neusten Patches und Updates installiert?
- Wurden unnötige Dienste entfernt?
- Wurden nicht verwendete Protokolle deaktiviert?
- Wurden nicht verwendete Dienst- und Benutzerkonten entfernt?
- Besteht eine restriktive Verwendung von Freigaben?
- Werden fehlgeschlagene Anmeldeversuche aufgezeichnet?
- Sind die Log-Dateien sicher vor fremdem Zugriff geschützt?
- Werden regelmässige Backups erstellt?
- Werden die Log-Dateien regelmässig überwacht?

6.1.8 Architekturbeispiele

- Wie sollen die Daten veröffentlicht werden? Wem zugänglich? Wie oft?
- Sollen die Daten nur angeschaut (read only) werden können?
- Wer muss die Daten von ausserhalb beschreiben können?
- Wie ist der Zugriff auf die Daten? VPN, Internet, LeasedLine?

- Was sind mögliche Argumente, dass ein Büro den GIS-Web-Server selbst betreibt? Oder eben nicht selbst betreibt?
- Welche Infrastruktur ist vorhanden?
- Welche Software-Lösungen sind vorhanden (Virenschutz, Authentifizierung, Verschlüsselung, etc)?
- Welche Komponenten (VPN-Server, GIS-Web-Server, Firewall, Produktions-Server) sind vorhanden?
- Welche Komponenten (VPN-Server, GIS-Web-Server, Firewall, Produktions-Server) sollen wo „aufgebaut“ werden?
- Welche Komponenten (VPN-Server, GIS-Web-Server, Firewall, Produktions-Server) müssen zwingend geschützt sein, welche nicht?
- Ist eine Aufteilung in Bereiche (mit versch. Logins) sinnvoll?

6.1.9 Realisierung

- Wo gibt es Beispiele im Umfeld?
- Gibt es Firmen/ Ämter/ Gemeinden in gleicher Grösse, die bereits eine Lösung haben?
- Wer sind die potentiellen Ansprechpartner für GIS-Web-Server Lösungen von Gemeinden und Ingenieurbüro?
- Was sind Aufgaben bei einer GIS-Web-Server Lösung, die ein Mitarbeiter der Gemeinde bzw. Ing. Büro übernehmen kann?
- Welche Vorkenntnisse sollte der interne Mitarbeiter mitbringen?
- Welches Budget steht zur Verfügung?

6.2 Literatur

- Bundesamt für Informatik, BFI (1993), Weisung Informatiksicherheit Nr. S01 (WS S01), Handhabung der Benutzeridentifikationen und der Passwörter
- Bundesamt für Informatik, BFI (1998), Weisung Informatiksicherheit Nr. S02 (WS S02), Grundschutz von Informatiksystemen und -anwendungen
- Bundesamt für Informatik, BFI (1997), Weisung Informatiksicherheit Nr. S03 (WS S03), Umsetzung der Network Security Policy (NSP)
- Chris Mahn (GSEC Version 1.2d, 21 May 2001), SANS Institute, Three Tiered DMZ's
- Computer Security Technology Center: http://www.ciac.org/cstc/
- Dave Peters (2003): System Design Strategies, An ESRI White Paper
- IT-Grundschutzhandbuch des deutschen Bundesamtes für Sicherheit: http://www.bsi.de/gshb/deutsch/menue.htm
- FBI Computer Crime Information: http://www.fbi.gov/
- Internet Society: http://www.isoc.org
- Informatikstrategieorgan Bund Schweiz SBI: http://www.isb.admin.ch/internet/sicherheit/00595/00596/index.html?lang=de
- Microsoft: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp
- Microsoft, Improving Web Application Security: Threats and Countermeasures
- National Security Agency: http://www.nsa.gov
- Raeplle, M. (2002): Sicherheitskonzepte für das Internet. Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung. dpunkt.verlag, iX Edition.
- Scott Young (Assignment Version 1.2b, March 26, 2001), SANS Institute, Designing a DMZ
- SNV, SN612010 Vermessung – Informationssicherheit – Sicherheit und Schutz von Geodaten
- Zehnder C. A. (2001): Informationssysteme und Datenbanken. 7. Auflage. Verlag der Fachvereine VdF
- Dr. Norbert Pollmann (3-8266-0988-3): Firewall Systeme

6.3 Glossar

Dieses Glossar stellt keinen Anspruch auf Vollständigkeit.

- Anonymität: Im Gegensatz zur Authentifikation schützt Anonymität eine Person davor, ihre Identität preiszugeben.
- Application-Server Server, auf dem bestimmte Applikationen, welche über das Intra-/ Internet verfügbar sein sollen, installiert sind.
- Authentifikation: Authentifikation meint die Überprüfung der Echtheit von Personen, Organisationen und Programmen.
- Daten-Server Dienst, welcher die Daten verwaltet
- DMZ: (DeMilitarized Zone): Bei einer DMZ ("Demilitarized Zone"/"entmilitarisierte Zone") handelt es sich um einen geschützten Rechnerverbund, der sich zwischen 2 Netzwerken befindet. Der Rechnerverbund wird jeweils durch einen Paketfilter gegen das dahinter stehende Netz abgeschirmt. Der Sinn des ganzen Aufwandes ist es, möglichst auf sicherer Basis Dienste des Rechnerverbundes sowohl dem einem als auch dem anderem Netz zur Verfügung zu stellen. Ein typisches Anwendungsbeispiel ist eine Firma, die einen eigenen Mailserver betreibt. Dieser Mailserver ist ein Teil der DMZ und muss natürlich von außen erreichbar sein, da ansonsten E-Mails nicht zugestellt werden könnten. Anderseits müssen auch die Clients, die am LAN angeschlossen sind, ihre E-Mails abholen. Deswegen brauchen auch sie Zugriff auf den Server [net-lexikon].
- http (Hypertext Transfer Protocol) Standardprotokoll, mit dem WWW-Dokumente vom Web-Server zum Browser übertragen werden.
- Integrität: Unter der Erhaltung der Integrität von Daten wird die Sicherung gegen beabsichtigte oder zufällige Manipulation verstanden [Raepple].
- IP Jeder an das Internet angeschlossene Rechner besitzt eine global eindeutige, 32 Bit lange numerische IP-Adresse. Um eine bessere Lesbarkeit zu erreichen werden IP-Adressen meist als 4 durch Punkte voneinander getrennte Bytes dargestellt - beispielsweise 134.100.11.181. Je nach ihrer Klasse bestimmen die ersten 1-3 Bytes einer IP-Adresse das Netzwerk, an den der Rechner angeschlossen ist, während die

	restlichen Bytes den Rechner in diesem Netzwerk identifizieren.
▪ Port	Um einzelne Anwendungen - sowohl Klienten als auch Server - auf einem bestimmten Rechner (Host) zu unterscheiden, werden sogenannte *Ports* verwendet. Jedem Port ist eine eigene *Portnummer* im Bereich von 1-65535 zugeordnet. Server verwenden meist eine wohldefinierte Portnummer <1024, an der sie auf Anfragen von Klienten warten. Die Standardportnummer für HTTP ist 80.
▪ Raid	Ein RAID-System (Abk. Redundant Array of Inexpensive / Independent Disks) dient zur Organisation von mehreren Festplatten bei einem Computer. Dadurch kann man Betriebssicherheit, Leistung und/oder Kapazität erhöhen. Dazu gibt es verschiedene Möglichkeiten, die man als RAID-Levels definiert hat.
▪ Replikation	siehe INTERLIS-Handbuch
▪ Spatial-Server	Dienst, welcher die Funktionen für die Behandlung von räumlichen Daten zur Verfügung stellt.
▪ SSL	SSL (Secure Socket Layer) ist ein Protokoll zur sicheren Kommunikation in TCP/IP-Netzwerken. Da SSL ein Protokoll auf Ebene der Transportschicht ist, können neben HTTP auch beliebige andere Protokolle der Anwendungsschicht, wie z.B. Telnet oder FTP, mit Hilfe von SSL abgesichert werden. SSL stellt den Applikationen einen sicheren Kanal zur Kommunikation über TCP-Verbindungen zur Verfügung. Die Verwendung von SSL ist für den Benutzer dabei weitgehend transparent.
▪ TCP	Das *Transmission Control Protocol* baut auf IP auf und überwacht den sicheren Transport der Daten. TCP ist ein verbindungsorientiertes Protokoll, d.h. vor der Übertragung der eigentlichen Daten wird erst eine so genannte *virtuelle Verbindung* aufgebaut. Übertragungsfehler werden von TCP automatisch korrigiert.
▪ TCP/IP	Die Kommunikation im Internet basiert auf der TCP/IP-Protokollfamilie. TCP/IP liegt - wie dem bekannten ISO/OSI Referenzmodell - eine Schichtenarchitektur zu Grunde. Zu den vier Schichten zählen neben der *Schnittstellenschicht*, die eine einheitliche Schnittstelle zur zugrunde liegenden Kommunikationshardware, wie z.B. *Ethernet* oder *Token Ring*, zur Verfügung stellt, die *Internetschicht* mit den Protokollen *IP* und *ICMP*, die *Transportschicht* mit den Proto-

kollen *TCP* und *UDP* und die Anwendungsschicht, die eine Vielzahl von Protokollen umfasst, unter anderem *HTTP*, *SMTP*, *FTP* und *Telnet*.

- Tier: engl. für Schicht
- Verfügbarkeit: Verfügbarkeit trifft Vorsorge dafür, dass nutzungsberechtigte Personen auf Information zur rechten Zeit und am rechten Ort zugreifen können. [Raepple].
- Vertraulichkeit: Vertraulichkeit schützt geheime Informationen beim Transport über das Internet vor unberechtigten Einblicken durch Dritte [Raepple].
- Web-Server (Oder "http-Server") Ein Server-Prozess läuft auf einer Web-Site, welche auf http-Anfragen anderer Server Antworten als Web-Seiten verschickt. Sind auf einer Web-Site mehr als ein Server installiert, müssen diese verschiedene Ports benutzen. Als Alternative können verschiedene Hostnamen auf den gleichen Rechner zeigen. In diesem Fall spricht man von „virtuellen Servern“.
- Zugriffskontrolle: Schutz gegen das unbefugte Eindringen in lokale Netzwerke bieten Zugriffskontrollen.

6.4 Abkürzungen

- DBMS Datenbank Management System
- DMZ: DeMilitarized Zone
- http Hypertext Transfer Protocol
- IP Jeder an das Internet angeschlossene Rechner besitzt eine global eindeutige, 32 Bit lange numerische IP-Adresse. Um eine bessere Lesbarkeit zu erreichen werden IP-Adressen meist als 4 durch Punkte voneinander getrennte Bytes dargestellt - beispielsweise 134.100.11.181. Je nach ihrer Klasse bestimmen die ersten 1-3 Bytes einer IP-Adresse das Netzwerk, an den der Rechner angeschlossen ist, während die restlichen Bytes den Rechner in diesem Netzwerk identifizieren.
- ISP Internet Service Provider
- LAN Local Area Network
- SSL Secure Socket Layer
- TCP Transmission Control Protocol

▪ TCP/IP	Die Kommunikation im Internet basiert auf der TCP/IP-Protokollfamilie. TCP/IP liegt - wie dem bekannten ISO/OSI Referenzmodell - eine Schichtenarchitektur zu Grunde. Zu den vier Schichten zählen neben der *Schnittstellenschicht*, die eine einheitliche Schnittstelle zur zugrunde liegenden Kommunikationshardware, wie z.B. *Ethernet* oder *Token Ring*, zur Verfügung stellt, die *Internetschicht* mit den Protokollen *IP* und *ICMP*, die *Transportschicht* mit den Protokollen *TCP* und *UDP* und die Anwendungsschicht, die eine Vielzahl von Protokollen umfasst, unter anderem *HTTP*, *SMTP*, *FTP* und *Telnet*.
▪ VPN	Virtual Private Network
▪ WAN	Wide Area Network