Ruhr-Universität Bochum
Fakultät für Elektrotechnik und Informationstechnik
Lehrstuhl für Kommunikationssicherheit
Seminar: IT-Sicherheit
Wintersemester 2002/2003

Sicherheit in Geoinformationssystemen

eingereicht am: 31.03.2003

Von: Benedikt Gierlichs
Matrikel-Nr.: 108 000 242347

Betreut durch: Prof. Dr.-Ing. Christof Paar

Kurzzusammenfassung

Obwohl der Begriff Geoinformationssystem bereits seit 1963 als Name für raumbezogene Datenverarbeitungssysteme verwendet wird, sind er und seine Bedeutung im Allgemeinen in der Bevölkerung unbekannt. Behörden und Unternehmen haben die Leistungsfähigkeit und den großen Nutzen dieser Systeme bereits vor vielen Jahren erkannt und setzen sie seitdem in zunehmendem Maße ein. Somit profitiert auch der Durchschnittsbürger schon seit einiger Zeit, wenn auch indirekt und unbemerkt, von Ihren Diensten. Selbst die bewußte Nutzung von Geoinformationssystemen wie z.B. öffentlich zugänglichen Routenplanern im Internet, wird meist noch als solche verkannt.

Auf Grund ihrer breit gefächerten Anwendungsmöglichkeiten werden Geoinformationssysteme heutzutage auf vielfältigen und äußerst unterschiedlichen Gebieten eingesetzt, die sich bis in den Bereich der kritischen Infrastrukturen erstrecken. Experten aus Politik, öffentlicher sowie privater Wirtschaft sind sich darüber einig, dass Geoinformationssysteme die Schlüsseltechnologie des 21. Jahrhunderts darstellen.

Im Verlauf dieser Arbeit werden Gefahrenpotenziale erläutert und anhand eines konkreten Beispiels Sicherheitslücken aufgedeckt. Das Ergebnis lautet daher, dass der Sicherheit in Geoinformationssystemen bisher viel zu wenig Aufmerksamkeit geschenkt wurde und akuter Handlungsbedarf besteht.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Motivation

Wir leben im postindustriellen Zeitalter, in dem Informationen zu den wichtigsten Wirtschaftsgütern zählen, wenn sie nicht sogar das wichtigste Wirtschaftsgut unserer Zeit darstellen. Wissensvorsprung kann für ein Unternehmen einen deutlichen Vorteil gegenüber Mitbewerbern bedeuten. Von den zahlreichen Wegen, Informationen zu gewinnen, seien hier die Erhebung und der Einkauf genannt. Mit Informationen wird wie mit klassischen Waren gehandelt - es existieren spezialisierte Unternehmen und Märkte. Eine weitere Möglichkeit an Informationen zu gelangen besteht daraus, vorhandene Daten auf eine neue Weise zu betrachten.

Geoinformationssysteme (GIS) ermöglichen solch eine neue Betrachtungsweise und haben sich in den letzten Jahrzehnten von einem exotischen Nischenprodukt zu einer völlig eigenständigen Technologie entwickelt, mit der sich ganze Wirtschaftszweige beschäftigen. Geoinformationen werden auf eigenen Märkten gehandelt und sind ein wichtiger Bestandteil öffentlicher und privatwirtschaftlicher Entscheidungsprozesse (Beipiele hierzu in Kapitel 4 ab Seite 16).

Ein großer Vorteil beim elektronischen Austausch von Daten ist ihr nicht materieller Charakter, der in Kombination mit den heutzutage vorhandenen Informationsinfrastrukturen und Datenverarbeitungsanlagen einen augenblicklichen Transfer sowie die sofortige Weiterverarbeitung im Zielsystem erlaubt. Die Schnelllebigkeit der vernetzten IT-Welt erzeugt allerdings auch eine gewisse Problematik: rasante Fehlerfortpflanzung. Störungen im Datentransferprozess zwischen Informationssystemen (IS) sollten daher von allen Beteiligten, wenn irgend möglich, ausgeschlossen, ansonsten schnellstmöglich aufgedeckt werden, da sie - spät erkannt - oft nicht mehr korrigierbar sind oder die Korrektur hohe Folgekosten mit sich bringt.

Zu den möglichen Ursachen solcher Störungen zählt auch absichtliches und böswilliges Handeln von Konkurrenten, Gegnern oder Neidern. Unsichere Kommunikationskanäle, wie beispielweise das Internet oder Funknetzwerke, stellen ein großes Sicherheitsrisiko dar und sind häufig Ansatzpunkt für Angriffe, deren Zielsetzung Datenmanipulation, unerlaubter Zugriff oder sogar Systemausfall lauten kann. Zumindest der Schutz der Daten ist mit Hilfe kryptographischer Methoden möglich, sofern sich die Verantwortlichen der Gefahren bewußt sind und entsprechend handeln.

Auch GISe sind auf Datenaustausch, der insbesondere bei mobilen Anwendungen über unsichere Kanäle abläuft, angewiesen.

1.2 Zielsetzung und Gliederung

Ziel dieser Arbeit war ursprünglich die Untersuchung der in GISen verwendeten Sicherheitsstandards. Bei den Recherchen ergab sich schnell, daß solche Standards bisher nicht geschaffen wurden, was beispielsweise auf die stark unterschiedlichen Einsatzgebiete und verwendeten Infrastrukturen zurückgeführt werden könnte.
Die vorliegende Arbeit soll auf diesen Mißstand aufmerksam machen und zeigen, daß in der Wachstumsbranche GISe bezüglich der Sicherheit großer Handlungsbedarf besteht. Dies umfasst sowohl eine Beschreibung der Funktionsweise der eingesetzten Systeme, als auch eine Analyse der Gefahrenpotentiale.

Die Arbeit zerfällt daher inhaltlich grob in zwei Teile. Die Kapitel 2,3 und 4 dienen der Einführung des Lesers in die Thematik. In Kapitel 2 wird durch die Festlegung einiger Begrifflichkeiten eine gemeinsame Ausgangsbasis geschaffen, die Missverständnissen vorbeugen soll. Kapitel 3 beschreibt die historische Entwicklung, Zukunftsaussichten, wirtschaftliche Relevanz und das Funktionsprinzip von GISen. Die in Kapitel 4 genannten Anwendungsbeispiele sollen dem Leser helfen, sein Verständnis von GISen zu vertiefen und ihm zeigen, wie vielfältig einsetzbar, mächtig und elegant sie sind.
In den Kapiteln 5 und 6 erfolgen die abstrakte und konkrete Analyse. Kapitel 5 ist der allgemeinen Gefahrenpotentialanalyse aus verschiedenen Blickwinkeln gewidmet. In Kapitel 6 wird zunächst ein reales Szenario vorgestellt und analysiert, später dann ein Angriff theoretisch durchgespielt.

2 Terminologie

Obwohl in der vorliegenden Arbeit ein Fachgebiet der Geographie und Themen aus dem Bereich der IT-Sicherheit behandelt werden, sollte es auch fachfremden Lesern möglich sein, sie zu verstehen. Die verwendeten Fachbegriffe werden entweder kontextuell oder in Fußnoten erläutert.
Einige Begrifflichkeiten erfordern jedoch eine etwas umfangreichere Beschreibung bzw. Festlegung, daher soll in diesem Kapitel zunächst eine gemeinsame Grundlage für die darauf folgenden Betrachtungen geschaffen werden.

2.1 Zeichen, Daten, Information und Wissen

Jede Niederschrift, ob analog oder digital, besteht aus Zeichenketten. Die Angabe einer Syntax, z.B. des Regelwerks der deutschen Grammatik, ermöglicht es, gültige Zeichenketten von Ungültigen zu unterscheiden (vgl. [Brockhaus98]). Unter Kenntnis der Syntax bezeichnet man Zeichenketten auch als Daten. Informationen unterscheiden sich von reinen Daten dadurch, daß sie kommuniziert werden und für den Betrachter bzw. Empfänger eine unmittelbare Bedeutung haben. Die Zuordnung eines bestimmten Sinnbildes zu einem Wort nennt man Semantik. (vgl. [Brockhaus98]). Werden Informationen kontextbezogen interpretiert, spricht man von Wissen. Die kontextuelle Vereindeutung eines Wortes ist Aufgabe der Pragmatik.

Abbildung 1: Zeichen, Daten, Information und Wissen

Folgendes Beispiel soll diese Zusammenhänge verdeutlichen:
Die Zeichenfolge 'Ich bin ein Affe.' beispielsweise hat zunächst keinerlei Wert. Durch Angabe der Syntax 'Deutsche Grammatik' wird daraus immerhin ein im Deutschen grammatikalisch korrekter Satz. Jede Person, der man die syntaktischen Regeln erklären würde, könnte dies bestätigen. Für eine der Deutschen Sprache mächtige Person, der dieser Satz mitgeteilt wird, ist er eine Information, da den einzelnen Wörtern eine Bedeutung zugeordnet werden kann und der Satz somit zu einer verständlichen Aussage wird. Denkt der Empfänger der Information kurz über diese nach, gelangt er zu Wissen, nämlich dem, daß sein Gegenüber entweder ein Lügner oder ein Evolutionswunder ist.

> „Information heisst [..] zweckorientiertes Wissen, vobei der Zweck in der Vorbereitung menschlichen Handelns liegt“[Brockhaus98].

Informationen helfen uns dabei, Entscheidungen zu treffen. Anders ausgedrückt treffen wir Entscheidungen auf Grund der uns vorliegenden Informationen. Die Suche nach Informationen ist also meistens darin begründet, Wissen über einflussnehmende Faktoren anzuhäufen, um darauf basierend zu entscheiden.

2.2 Informationssystem

Ein Informationssystem (IS) besteht aus einer Menge von Informationen und einem zugrundegelegten Ordnungsschema, das jede Information eindeutig identifiziert und es dem Benutzer des Systems ermöglicht, effektiv auf den Informationsbestand zuzugreifen.

2.2.1 Analoge Informationssysteme

Die Idee des ISs ist nicht von gestern, sie ist viele tausend Jahre alt. Schon die alten Ägypter hatten die Vorteile der Speicherung von Informationen durch Niederschrift erkannt und meisselten ihre Hieroglyphen zunächst in Stein. Später, nach der Erfindung des Papyrus, erfolgte die Niederschrift dann je nach Zweck auch auf diesem Medium. Selbst im letzten Jahrhundert waren ISe auf Grund der nicht vorhandenen Technologie meist analoge Systeme, bei denen Informationen auf Papier gespeichert wurden und durch sinnvolle Sortierung schnell auffindbar waren. Als Beispiele sollen hier der Karteikasten, das Telefonbuch und das Lexikon genügen.
Einige Schwachstellen dieser Systeme lassen sich leicht erkennen:

- geringe Informationsdichte auf dem Speichermedium, da die Informationen menschenlesbar abgelegt werden müssen, damit einhergehend hoher Platzbedarf (z.B. Bibliotheken)
- hohe Zugriffszeiten auf einzelne Informationen
- Einfügen, Ändern und Löschen von Informationen nur mit großem Aufwand möglich
- Gefahr des Verlustes der Übersichtlichkeit (in welchem Buch schlägt man nach?)

- keine Kreuzverknüpfungen - stößt man z.B. bei der Recherche in einem Lexikon auf einen unbekannten Begriff, so muß man diesen ebenfalls, eventuell in einem anderen Buch, nachschlagen

2.2.2 Digitale Informationssysteme

Die Fortschritte in der Computertechnologie ermöglichten die Entwicklung der digitalen, rechnergestützten ISe, die in nahezu allen Belangen wesentlich effizienter als ihre Vorgänger sind. Moderne digitale ISe ermöglichen durch ihre Komplexität und Leistungsfähigkeit die schnelle Verarbeitung wahrer Informationsberge und leisten in Sekunden, was von Menschenhand nicht in Jahren zu bewältigen wäre. Sie speichern die erfassten Informationen in Datenbanken (z.B. MYSQL[1], Oracle[2]), die die Verwaltung übernehmen und den Zugriff über definierte Schnittstellen ermöglichen (z.B. SQL[3]), erlauben umfangreiche Manipulationen und Analysen sowie die Ausgabe von Ergebnissen. Einige der offensichtlichen Vorteile sind:

- hohe Informationsdichte auf dem Speichermedium (ganze Enzyklopädien auf einer CD-ROM)
- geringe Zugriffszeiten
- problemlose Manipulation und Migration einzelner Informationen oder ganzer Datenbanken
- Keuzverknüpfungen sogar in andere ISe problemlos realisierbar

[1] Open Source Datenbank - http://www.mysql.com
[2] Kommerzielle Datenbank - http://www.oracle.com
[3] Standard Query Language

Als Beispiel für die Leistungsfähigkeit solcher Systeme sei hier die Internetsuchmaschine Google genannt.

> „Google erreicht über 2,0 Milliarden Web-Seiten und liefert in meist weniger als einer halben Sekunde relevante Suchergebnisse an Benutzer in aller Welt. Im Augenblick beantwortet Google mehr als 100 Millionen Anfragen pro Tag“[GoogleInc].

Ein einfaches Anwendungsbeispiel digitaler ISe stellt der Download des Aushangfahrplans von einer bestimmten Haltestelle und Linie im öffentlichen Nahverkehr dar. Dies ist für NRW unter `http://www.bus-und-bahn.de/ocx2.exe?GP=48` nach einem Klick auf 'Aushangfahrplan', der Auswahl der Haltestelle sowie der Linie und Richtung möglich. Nach einigen Sekunden erhält der Benutzer Auskunft darüber, wann das gewünschte Verkehrsmittel an seiner Haltestelle in die gewünschte Richtung abfährt. (Die Komplikationen des Umsteigens werden an dieser Stelle bewusst vernachlässigt, allerdings wird ein wenig später auf sie eingegangen.)

Besonders in zeitkritischen oder datenintensiven Anwendungen verlassen wir uns heutzutage völlig auf die fehlerfreie Funktion der zugrundeliegenden digitalen ISe und sind von Ihnen abhängig, da sie auf Grund ihrer Komplexität nicht durch analoge Systeme zu ersetzen sind.

2.2.3 Kritische Infrastrukturen

Der Einsatz von digitalen ISen in den sogenannten kritischen Infrastrukturen ist von ganz besonderer Bedeutung. Als kritische Infrastruktur bezeichnet das Bundesamt für Sicherheit in der Informationstechnik Organisationen oder Einrichtungen von (lebens-) wichtiger Bedeutung für das staatliche Gemeinwesen und nennt in diesem Zusammenhang

- Telekommunikation
- Transport- und Verkehrswesen
- Energieversorgung
- Gesundheitswesen

- Notfall- und Rettungsdienste
- Regierung und öffentliche Dienste
- Bank-, Finanz- und Versicherungswesen

als Beispiele. Bei Ausfällen oder Störungen kommt es zu nachhaltig wirkenden, dramatischen Folgen für größere Bevölkerungsgruppen (vgl. [BSI]). Diese können insbesondere aus (absichtlich herbeigeführten) Fehlfunktionen der zugrundeliegenden Informationstechnologie (IT) bzw. ISe resultieren. Fortschritt und Wohlstand unserer Gesellschaft basieren nicht zuletzt auf IT, von der wir abhängig sind und die uns, da es keinen 100%igen Schutz gibt, verletzlich macht.

2.3 Geoinformationssysteme

> „Ein Geographisches Informationssystem bezeichnet ein rechnergestütztes System, das aus Hardware, Software, Daten und Anwendungen besteht. Mit ihm können raumbezogene Daten digital erfasst und redigiert, gespeichert und reorganisiert, modelliert und analysiert sowie alphanumerisch und graphisch präsentiert werden“[Bill91].

Geographische Informationssysteme, kurz Geoinformationssysteme (GIS), unterscheiden sich von anderen ISen durch eine grundlegende Eigenschaft: Die in Ihnen gespeicherten Informationen sind mit ihrem Raumbezug verknüpft, so dass Abfragen unter Einbezug räumlicher Aspekte möglich sind (vgl. [Linder99]). Auf der anderen Seite unterscheiden sich GISe von reinen Kartier- oder CAD Systemen durch ihre Analysefähikeit, sie können verknüpfte Sachdaten (siehe Kapitel 3.3 ab Seite15) verarbeiten (vgl. [Muhar92]).
Das Grundprinzip von GISen kann sehr gut durch das Bild einer mit Stecknadeln und Fähnchen gespickten Landkarte verdeutlicht werden, wie es aus älteren Kriminalfilmen bekannt sein dürfte. Hier wurden z.B. Tatorte (Sachdaten) durch Stecknadeln repräsentiert und ihr räumlicher Bezug durch einstecken der Nadeln an korrekter Position auf einer Landkarte visualisiert. So standen völlig neue Analysemethoden zur Verfügung.
Auch die Umsteigeproblematik aus dem Beispiel des ÖPNV (s.o. Kapitel 2.2.2) lässt sich hervorragend einsetzen, um die Idee hinter GISen zu vermitteln.
Nur anhand von Fahrplänen eine Fahrt mit mehrfachem Umsteigen durch eine unbekannte Stadt zu planen ist offensichtlich ein größeres Vorhaben, da zu benutzende Linien und

geeignete Umsteigepunkte herausgesucht werden müssen. Eine große Hilfe bietet hier ein Stadtplan, auf dem Haltestellen und Linienverläufe (Sachdaten) an korrekter Stelle markiert bzw. skizziert sind (Raumbezug).

3 Einführung in GISe

3.1 Historie und Zukunft

Der Begriff Geographisches Informationssystem wurde 1963 von R.F. Tomlinson bei der Einrichtung eines rechnergestützten, raumbezogenen Informationssystems eingeführt. Er entwickelte im Auftrag der kanadischen Regierung Anfang der 60er Jahre das Canadian Geographical Informations System (CGIS), dass im Rahmen eines Programms zur Förderung von Landwirtschaft und Umweltschutz Landnutzungsinformationen verarbeiten und analysieren sollte.
Landschafts- und Umweltplaner trieben die Entwicklung von GIS in den 60er Jahren voran. Nordamerikanische Staaten förderten Anfang der 70er Jahre die Entwicklung von Kartographie-Programmen, die bereits Funktionen heutiger GIS aufwiesen, insbesondere für militärische Zwecke. Diese Systeme wurden vor allem zur flugzeug- und satellitengestützten Landvermessung eingesetzt, da somit Karten mit direktem Bezug zu Fernerkundungsdaten erstellt werden konnten (vgl.[Borrough86]).
Die Fortschritte der GIS wurden aber von ihrer Erfindung an bis in die späten 80er Jahre insbesondere von Landschafts- und Umweltplanern (natürliche Ressourcen, Umweltbelastungen, usw.) herbeigeführt.
Da die anfallende Informationsmenge zur damaligen Zeit nur von extrem teuren Großrechenanlagen bewältigt werden konnte, blieb die Nutzung solcher Systeme lediglich einem kleinen Personenkreis vorbehalten - an eine breite praktische Anwendung war nicht zu denken. Durch die rasante Entwicklung der Computertechnologie wurde der Einsatz von GISen zu Beginn der 90er Jahre jedoch in größerem Umfang möglich. Seitdem nimmt der Einsatz von GISen sowohl in Behörden als auch in der Privatwirtschaft zu.
(Unter `http://www.casa.ucl.ac.uk/gistimeline/` kann der interessierte Leser, nach Auswahl einiger Kriterien, die Entwicklung von GISen anhand einer Zeitlinie betrachten.)
In den letzten Jahren haben immer mehr Behörden und Unternehmen die Vorteile der leistungsfähigen GISe erkannt. Im öffentlichen Sektor werden GISe beispielsweise zur Landschafts-, Raum- und Versorgungsnetzplanung sowie für Umweltbelastungsanalysen und -Schutz eingesetzt. Die zahlreichen Anwendungen von GISen in der Privatwirtschaft seien hier zunächst unter dem Oberbegriff Business Mapping zusammengefasst, da auf sie später im Detail eingegangen wird.

Die zukünftigen Anwendungsmöglichkeiten für GISe sind vielfach und facettenreich – scheinbar unbegrenzt. Zahlreiche Experten sind sich darüber einig, daß GISe nicht nur eine IT-Anwendung, sondern die Schlüsseltechnologie des 21. Jahrhunderts darstellen. Bund und Länder haben das Potenzial von GISen erkannt und führen in nationalen und internationalen Kooperationen, auch mit der EU, verschiedene Initiativprojekte durch. Das Land NRW fördert beispielsweise mit seiner Initiative gdi-nrw[4], den Aufbau einer nationalen GeoDatenInfrastruktur. Ziel ist es, den Markt für Geoinformationen zu öffnen und auszubauen.
Dies ist auch die Zielsetzung der Initiative Geoinformationswirtschaftskongreß[5], die vom Bundesministerium des Innern, dem Land NRW und der Initiative D21[6], dem größten private-public-partnership in Deutschland, getragen wird.

3.2 Wirtschaftliche Relevanz

Die wirtschaftliche Relevanz von GISen soll anhand der folgenden Zahlen verdeutlicht werden:
In einer von der EU in Auftrag gegebenen Studie aus dem Jahr 2000 wird das europaweite Potenzial für Informationen des öffentlichen Raumes mit 68,2 Mrd. Euro beziffert. Dieser Wert setzt sich aus 35,8 Mrd. Euro für Geoinformationen, also heute schon durch GISe nutzbaren Informationen, und 32,4 Mrd. Euro für noch nicht verortete Sachdaten, die zur Zeit nicht durch GISe nutzbar sind, zusammen (vgl. [EU-Studie00]).

Das Potenzial des deutschen Geoinformationsmarktes wird in einer vom Bundesministerium für Wirtschaft und Arbeit in Auftrag gegebenen Studie mit rund 8 Mrd. Euro angegeben, wovon derzeit maximal 15%, also 1,2 Mrd. Euro, genutzt werden. 80 bis 90% der öffentlichen Daten haben einen konkreten Bezug zum Raum und sind verortbar, wären also durch GIS nutzbar (vgl. [MICUS03]). Bereits im Jahr 1999 wurde weltweit GIS-Software im Wert von 845 Millionen US$ umgesetzt (vgl. [Daratech00]).

Selbst vorsichtige Schätzungen von Experten sagen überdurchschnittliche Wachstumsraten des Geoinformations-Marktes voraus. In den USA, die schon viele Anfangsprobleme gelöst haben, vor denen Deutschland noch steht, wurden in den letzten Jahren Wachstumsraten des Geoinformations-Marktes zwischen 11 und 37% erreicht (vgl. [MICUS03]).

[4] http://www.cegi.de, http://gdi-nrw.uni-muenster.de
[5] http://www.geoinformationswirtschaft.de
[6] http://www.initiatived21.de

3.3 Das Prinzip

Der schematische Aufbau eines GIS kann aus funktionsbezogener Sichtweise mit vier Einheiten beschrieben werden.

Abbildung 2: Schematischer Aufbau eines GISs

Das Backend eines GISs bilden eine oder mehrere Datenbanken, die die Daten des Systems beinhalten und verwalten. Man unterscheidet typischerweise drei Datentypen:
Geobasisdaten sind die Träger aller anderen Daten und werden deshalb zuerst genannt. Unter Geobasisdaten versteht man u.a. amtliche topographische Karten, wie sie von Vermessungsämtern erstellt werden, Luftbildphotos und Satellitenaufnahmen. Allgemein kann man sagen, dass Geobasisdaten die Erdoberfläche beschreiben.
Einen anderen Datentyp stellen geokodierte Daten dar. Zum Verständnis sei zunächst der Begriff Geokodierung (oder Georeferenzierung) erläutert. Mit Geokodierung wird der Vorgang beschrieben, bei dem einem realen Objekt ein konkreter Bezug zum Raum zugeordnet wird, so dass dieser auf einer Lankarte abgebildet werden kann. Dieser Vorgang kann je nach Bedarf in verschiedenen Auflösungen, vom Postleitzahlgebiet bis hin zur Genauigkeit von Hausnummern, erfolgen und bedeutet i.d.R. das Zuordnen von Koordinaten zu einem Objekt. Unter geokodierten Daten versteht man eindeutig identifizierbare Objekte der realen Welt, die mit ihrem Raumbezug verknüpft sind. Als Beispiel diene hier ein fiktives Haus in der Mustergasse 1 in 12345 Musterstadt, dem seine genaue geographische Lage zugeordnet ist.
Sachdaten stellen den dritten Datentyp dar. Als Sachdaten bezeichnet man Daten, die nicht in direktem Bezug zum Raum stehen, wie z.B. Statistiken und Meßwerte. Sachdaten werden beispielweise von statistischen Ämtern, Umweltschutzorganisationen und Marktforschungsunternehmen erhoben und eventuell angeboten. Ein mögliches Beispiel ist die Kenntnis darüber, dass in besagtem Haus in der Mustergasse ein Blumengeschäft ist.

Abfrage- oder Analysetools bilden eine weitere Funktionseinheit eines GIS. Sie kommunizieren über definierte Schnittstellen (z.B. SQL) mit den Datenbanken und übernehmen das Zusammentragen der gewünschten Informationen.

Das Interface ist die Einheit, die den Kommunikationsfluß zwischen Benutzer und Analysetool steuert und überwacht. Es nimmt die Anfragen des Clients entgegen, leitet diese an

das Analysetool weiter, nimmt die Ergebnisse entgegen, überarbeitet sie eventuell und schickt sie schließlich an den Client. Gängige Interfaces sind Spezialsoftware, die bestimmte Clients erfordern und Webinterfaces, die, wenn meist auch weniger spezifisch, offener einsetzbar sind.

Das Frontend bzw. der Client ist die Einheit eines GISs, die für den Benutzer sichtbar ist - die Benutzerschnittstelle. Das Frontend ist i.d.R. eine Software, die es dem Benutzer des Systems ermöglicht Analysen zu erstellen und ihm die Ergebnisse alphanumerisch bzw. graphisch präsentiert. Gängige Frontends sind vor allem Spezialsoftware (in Verbindung mit Spezialinterfaces) und sogenannte Light-Clients, die in Webbrowsern ablaufen. In den letzten Jahren hat sich ein Trend hin zu mobilen Clients abgezeichnet, der sich auch in Zukunft fortsetzen, wahrscheinlich sogar verstärken wird. Unter mobilen Clients versteht man Software, die auf mobilen Geräten wie z.B. Mobiltelefonen, PDAs[7] oder Navigationsgeräten ausgeführt wird.
Der Datenaustausch zwischen Client und Interface erfolgt bei stationären Systemem meist über firmeninterne Netzwerke und/oder das Internet. Mobile Clients nutzen je nach Anwendung Mobilfunknetze, wie beispielsweise GSM[8], GPRS[9], EDGE[10], oder zukünftig auch die 3G[11] Netze 3GSM und UMTS[12], empfangen ihre Daten über RDS[13], das von Radiostationen ausgestrahlt wird, oder nutzen WLAN[14]-Technologie.

4 Anwendungsbeispiele

Bevor im weiteren vier konkrete Anwendungsbeispiele erörtert werden, soll nochmals aufgezeigt werden, in welchem Maße GISe die Informationsanalyse und -Aufbereitung revolutionieren, indem sie neue Betrachtungsweisen ermöglichen.

Gegeben sei die Fragestellung: *Wie sieht die Bevölkerungsverteilung in den Postleitzahlbezirken des Ruhrgebiets aus?* Diese Information könnte zur Entscheidung über den Standort einer neuen Filiale gebraucht werden.

[7] Personal Digital Assistant
[8] Global System for Mobile communications
[9] General Packet Radio Services
[10] Enhanced Data for GSM Evolution
[11] Third Generation
[12] Universal Mobile Telephone System
[13] Radio Data System
[14] Wireless Local Area Network

Ohne GISe könnte die Antwort in Form einer Tabelle gegeben werden, die die einzelnen Postleitzahlbezirke, die Bevölkerungsanzahl, die Fläche des Gebiets und die daraus resultierende Bevölkerungsdichte enthält. Obwohl diese Tabelle die gewünschte Information enthält, ist sie offensichtlich nicht dazu geeignet, sie darzustellen. Benachbarte PLZ-Bezirke sind beispielsweise nicht erkennbar - der Tabelle fehlt der räumliche Bezug. Mit einem GIS läßt sich die Fragestellung wesentlich eleganter beantworten. Die gewünschte Information könnte durch eine Karte visualisiert werden, in der die verschiedenen PLZ-Bezirke entsprechend ihrer Bevölkerungsdichte eingefärbt sind. Ballungsräume würden so auch über PLZ-Grenzen hinweg erkennbar, was einer wesentlich realistischeren Darstellung entspricht.

In Bezug auf räumliche Fragestellungen sagt eine Karte oft mehr als tausend Worte, wie gerade gezeigt wurde.
GISe stellen neue, mächtige Visualisierungs- und Analysemethoden zur Verfügung (vgl. [Schmidt02]).

Wie bereits in Kapitel 3.1 ab Seite 13 erläutert wurde, werden GISe sowohl auf behördlicher Seite als auch von Unternehmen eingesetzt. Es liegt nahe, daß der unternehmerische Einsatz von GISen unter dem Aspekt der wirtschaftlichen Relevanz eine wesentlich größere Tragweite hat, da hier i.A. Umsatz- und Gewinnsteigerungsabsichten unterstellt werden können. Aus diesem Grund werden sich alle folgenden Betrachtungen auf diesen Bereich begrenzen.
Es ist Common Sense, dass ca. 80% der unternehmerischen Fragestellungen einen konkreten Raumbezug haben, so dass der Einsatz von GISen unerlässlich scheint (vgl. [Schmidt02]).

Business Mapping ist der Oberbegriff, unter dem die verschiedenen Anwendungsgebiete von GISen in der Wirtschaft zusammengefasst werden, dies sind beispielweise:

- Routing
- Geomarketing (Markt- und Kundenanalysen)
- Standortmanagement (Einzugsgebiete, Verkehrsanbindung)
- Logistik (Lagerverwaltung, Tourenplanung)
- Facility Management

4.1 Routing

Die wohl bekannteste Anwendung von GISen, wenn auch meist nicht als solche erkannt, sind die Routing-Anwendungen. Diese sind z.B. in der Lage, unter Beachtung bestimmter von dem Benutzer vorgegebenen Einschränkungen, kürzeste oder schnellste Wege zwischen zwei oder mehr Orten zu bestimmen und je nach Wunsch des Anwenders tabellarisch oder graphisch auszugeben. Im Internet werden zahlreiche Routenplaner, teilweise sogar als Gratisdienste, angeboten, die auf solchen GIS-Anwendungen basieren. In Kombination mit einem GPS-Empfänger[15] kann eine solche Routing-Anwendung zu einem Navigationssystem ausgebaut werden, wie sie heute schon häufig in Kraftfahrzeuge eingebaut oder als mobile Geräte mitgeführt werden.

4.2 Geomarketing - Marktanalysen

In diesem Beispiel wird der Einsatz von GISen zu Marktanalysezwecken erläutert und gezeigt, wie effizient sich dadurch auch komplexe Fragestellungen beantworten lassen. Hierzu diene uns Unternehmer A, der sich fragt, wie die Relation zwischen Kaufkraftpotential und tatsächlich erzeugtem Umsatz seiner Kunden in den einzelnen Landkreisen Deutschlands aussieht.
A lässt zunächst die Adressdaten seiner Kunden von einem externen Dienstleister auf Landkreiszugehörigkeit geokodieren, damit sie vom GIS verarbeitet werden können. Die Umsatzzahlen der einzelnen Kunden entnimmt A seiner Buchhaltung, die Zahlen zu

[15] GPS = Global Positioning System

Kaufkraftpotentialen erhebt er entweder selbst oder kauft sie von extern ein.
Die Bildung der Relation 'Umsatz im Verhältnis zu Potential' erlaubt nun eine erste Aussage darüber, wie sehr ein Kunde an A gebunden ist. Durch Zusammenfassen naher

Abbildung 3: Business Mapping - Markanalysen, Quelle: [Fecht]

Relationen in geeignete Klassen, lässt sich ein übersichtliches Maß bilden. Jeder Landkreis kann nun in eine der Klassen eingeordnet werden. Das Ergebnis dieser Zuordnung kann anhand einer Karte, auf der die einzelnen Landkreise gemäß der zugeordneten Klasse eingefärbt werden, elegant dargestellt werden. Die Darstellung des Ergebnisses in tabellarischer Form wäre ohne Zweifel weniger übersichtlich und aussagekräftig.

4.3 Logistik - Container-Terminal Altenwerder im Hamburger Hafen

In diesem Beispiel wird die vollautomtische Bewirtschaftung eines Großlagers erläutert. Es wurde ausgewählt, um aufzuzeigen, dass positionsbezogene Daten auch in logistischen Fragestellungen große Bedeutung haben.

Mitte 2002 wurde im Hamburger Hafen der erste Teil des seit 1996 im Bau befindlichen Container-Terminals Altenwerder (CTA) von der Betreibergesellschaft CTA GmbH in Betrieb genommen. Die Fertigstellung des CTA, der von der Hamburger Hafen- und Lagerhaus AG zusammen mit Hapag-Lloyd gebaut wird, ist für Mitte 2004 geplant - dann wird er der größte und modernste Container-Terminal Europas sein. Um die Dimensionen dieses Projekts zu verdeutlichen, seien hier einige Zahlenwerte angegeben, die teilweise den Stand ab Mitte 2004 widerspiegeln.
Auf einer Kailänge von 1400m können bis zu vier Großcontainerschiffe gleichzeitig von insgesamt 14 Containerbrücken be- und entladen werden. Jedes Schiff dieser Kategorie kann mehr als 6000 Standard-Container, TEU[16] genannt, laden. Von der ca. 200ha grossen Nutzfläche des gesamten Hafenteils entfallen 225000m^2 auf das Containerlager, das bis zu 30000 TEU fassen kann. Der geplante Umschlag beläuft sich auf 1,9 Mio TEU pro Jahr, die Gesamtinvestitionskosten betragen etwa 670 Mio DM.

Abbildung 4: Modell des CTA, Quelle: [Hartmann02]

[16] TEU = Twenty feet Equivalent Unit: 20' * 8' * 8' ~ 6,1m * 2,4m * 2,4m

Um die geplanten Zahlen zu realisieren setzen die Erbauer und Betreiber auf modernste und hochgradig automatisierte Logistiksysteme. So erfolgt die Verwaltung und Bewirtschaftung des Containerlagers ohne menschliche Eingriffe, selbst das Be- und Entladen von Schiffen, Zügen und LKWs erfolgt größtenteils automatisch oder ferngesteuert.
Das Lager ist in 22 Blöcke ($10 * 37 * 4$ Container) aufgeteilt, die jeweils von zwei vollautomatischen Kränen (RMG[17]) bedient werden. Den Transport der Container zwischen Kaimauer und Lagerblöcken übernimmt eine Flotte von bis zu 65 Transportfahrzeugen (AGV[18]), die auf der 100m tiefen und für Personen komplett gesperrten Verkehrsfläche vollautomatisch agieren und sich an im Boden verlegten elektronischen Marken orientieren.

Abbildung 5: Automated Guided Vehicle, Quelle: [HHLA]

Die Vergabe von Aufträgen an die einzelnen Geräte erfolgt über die Terminallogistik und -Steuerung (TLS).

> „Auf Grund des hohen Automatisierungsgrades der einzelnen logistischen Abläufe kommt der TLS eine herausragende Bedeutung für die Produktivität des Gesamtterminals zu“ [Schü-Ha].

Das Optimierungsproblem der Auftragszuordnung durch die TLS ist die zeitliche Koordinierung der Übergaben zwischen den verschiedenen Geräten. Für jeden Auftrag wird aus der Menge der verfügbaren Geräte die Kombination ausgewählt, die unter der Bedingung der Minimierung von Wartezeiten, Leerfahrten und Verspätungen optimal erscheint. Die Zuordung der Aufträge erfolgt dabei online und dynamisch, um auch auf kurzfristige Änderungen, wie z.B. neue Aufträge, reagieren zu können.
Grundlage des Zuordnungsprozesses sind Verfügbarkeit und Position der Geräte sowie die Vorgabezeiten.
Auch nach der Auftragsvergabe sind aktuelle Positionsdaten der einzelnen Geräte enorm wichtig, da sich das Gesamtsystem nur mit Ihrer Kenntnis unfallfrei steuern läßt.
Quellen: [HHLA, HH02, Hartmann02, Schü-Ha]

[17] Rail Mounted Gantry crane
[18] Automated Guided Vehicle

4.4 Anwendungen in kritischen Infrastrukturen

GISe werden auch in Kritischen Infrastrukturen (siehe Kapitel 2.2.3 ab Seite 10) eingesetzt, was anhand der folgenden, kurzen Beispiele gezeigt werden soll.

Zunächst wird unterschieden, in welchem Maße die Kritische Infrastruktur in ihrer Funktion direkt vom GIS abhängig ist. Als Beispiel für Echtzeitabhängigkeit werden hier Notfall- und Rettungsdienste genannt. Dass Verkehrs- und Transportwesen auf aktuelle Positionsdaten angewiesen sind, wurde bereits exemplarisch im vorherigen Kapitel gezeigt. Auf indirekt abhängige Kritische Infrastrukturen wird danach am Beispiel der Energieversorgung eingegangen.

GISe helfen bei der Rettung von Menschenleben, indem sie beispielsweise Polizei, Feuerwehr oder THW bei ihrer Arbeit unterstützen. Die Rettungsleitstellen setzen GISe zur Fahrzeugnavigation, Standortbestimmung und Einsatzplanung ein (vgl. [Flyer]). Dies bedeutet im Einzelnen insbesondere die Auswahl schnellstmöglich verfügbarer Ressourcen, wie z.B. Fahrzeugen, anhand ihrer Position und ihres Status sowie die Ermittlung einer günstigen Route zum Einsatzgebiet.

Energieversorger benutzen früher schematische Anlagenpläne und Karten für die Netzdokumentation. Die heutzutage eingesetzten GISe erleichtern diese Arbeit immens und bieten zusätzliche Anwendungsmöglichkeiten. Neben der Dokumentation des Ist-Zustandes eines Netzwerks erleichtern GISe beispielsweise Investitionsentscheidungen bezüglich des Netzausbaus sowie die Netzverwaltung und helfen bei Störungsanalysen (vgl. [repasAEG]).

5 Gefahrenpotentialanalyse

Durch die Beispiele wurde gezeigt, dass GISe nicht mehr nur eine exotische Idee sind, sondern dass sie ganz im Gegenteil in der realen Praxis alltäglich eingesetzt werden. Selbst der vielleicht technisch unbedarfte Normalbürger nutzt, eventuell auch unbemerkt, ihre Dienste, profitiert aber in jedem Fall davon, dass Unternehmen und Behörden sie einsetzen.

Dieses Kapitel wird sich mit der Analyse des Gefahrenpotentials beschäftigen, d.h., es wird untersucht werden, ob Gefahrenpotential überhaupt vorhanden ist, oder ob mit dieser Arbeit nur „die Pferde scheu gemacht werden".
Bereits vor dem eigentlichen Einstieg in die Materie lassen sich zwei Indikatoren für das Vorhandensein von Gefahrenpotential ausmachen.
Zum Einen ist dies die Tatsache, dass der Einsatz eines GISs i.d.R. Datenaustausch mit mindestens einer anderen Partei erfordert. Abhängig vom Typ (siehe Kapitel 3.3 ab Seite 15) haben die ausgetauschten Daten für den Nutzer einen stark unterschiedlichen Wert, insbesondere können die Sachdaten extrem wertvoll sein.
Es wird davon ausgegangen, dass sich der Leser darüber bewusst ist, dass, wo immer es um große Werte geht, die Gefahr von Missbrauch und Betrug gegenwärtig ist. Man stelle sich nur vor, welcher Schaden für ein Unternehmen entsteht, dessen Kundenstamm einem Konkurrenten zugänglich gemacht wird.
Zum Anderen ist der Datenaustausch an sich, der teilweise online geschieht, ein Indiz. Insbesondere mobile Clients sind auf den Online-Datenaustausch mit Providern angewiesen, da sie nicht über die notwendigen Speicher- und Rechenkapazitäten verfügen, um autonom zu funktionieren. Mobile Clients nutzen, wie in Kapitel 3.3 ab Seite 15 beschrieben wurde, überwiegend Funknetze, die bisher als besonders leicht angreifbar gelten (vgl. [Bley02]), aber auch der Datenaustausch über das Internet ist zunächst, wie leider oft verkannt wird, nicht sicher (vgl. [BSI3]).

Im Folgenden wird das Gefahrenpotential aus den drei unterschiedlichen Sichtweisen von

- Content Providern
- Service Providern
- Kunden / Nutzern

betrachtet.

5.1 Content Provider

Der Content Provider bietet seine Daten (Geobasisdaten, Sachdaten) bzw. Nutzungsrechte daran oder Datenveredelungsdienste (Geokodierung) öffentlich an. Man kann davon ausgehen, dass die Gewinnung dieser Daten durch Erhebung, Vermessung o.ä. mit hohen Investitionskosten verbunden war. Gleiches gilt für die permanente Aktualisierung dieser Daten. Bisher gibt es für die zur Nutzung zur Verfügung gestellten Daten keinen standartisierten Schutz, wie z.B. durch starke Kryptographie. Der Content Provider ist hier mit den gleichen Problemen konfrontiert, wie alle Anbieter digitaler Medien. Die Problematik der Raubkopie ist besonders im Bereich digitaler Multimedia-Angebote, wie Filmen auf DVDs oder Musik auf Audio-CDs, prägnant – die dadurch erzeugten Verluste für Film- und Musikindustrie sind nicht mehr zu vernachlässigen.

Das Stichwort lautet hier Content Protection und sollte zumindest bei „Crypto-Insidern“ den Begriff Digital Rights Management ins Bewußtsein rufen.
Es exisiteren zwar bereits einige proprietäre Lösungen, um den Schutz der Daten sicherzustellen, doch kann erst das Schaffen von Standards einen umfassenden globalen Schutz bieten, der auch bei wechselnden Vertragspartnern greift.

5.2 Service Provider

Der Service Provider soll hier als Technik-Partner verstanden werden, er stellt die zur Abwicklung der Kommunikation erforderliche Infrastruktur zur Verfügung. Diese Infrastrukturen können beispielsweise firmeninterne Netze, Internetzugänge, Funknetze oder Sendestationen für Radiosignale sein, wie sie von ISPs[19], Mobilfunknetzbetreibern oder Radiosendern zur Nutzung angeboten werden. Es ist auch denkbar, dass der Service Provider das Hosting für eine komplette, webbasierte GIS-Platform in seinem Rechenzentrum übernimmt. Im weitesten Sinne können sogar Post- oder Paketdienste als Service Provider verstanden werden, da der Austausch größerer Datenmengen per CD nicht unüblich ist.

Während des Transfers der Daten vom Anbieter zum Nutzer ist der Service Provider für den Schutz, insbesondere aber generell für die Verfügbarkeit der Daten, verantwortlich. (Herbeigeführte) Netz- oder Systemausfälle sowie die Verfälschung der Daten während des Transfers führen neben eventuellen Konventionalstrafen zu starken Imageverlusten.

[19] Internet Service Provider

Die Vertrauenswürdigkeit des Anbieters sinkt, was zu Kundenabwanderung und finaziellen Einbußen führen kann.

IT-Sicherheitskonzepte, die Netz- und Systemsicherheit im Sinne von Security, Safety und Datensicherheit umfassen, können hier helfen, Risiken und eventuelle Verluste zu minimieren.

5.3 Kunde / Nutzer

Zunächst sei erläutert, auf wen diese Sichtweise zutrifft. Als Kunden oder Nutzer verstehen sich Endnutzer, die ein GIS zur Informationsgewinnung einsetzen und Zwischenhändler, die Daten einkaufen, um diese dann durch GISe nutzbar anzubieten (öffentlich oder firmenintern). Im Weiteren wird der Begriff Kunde stellvertretend für beide Gruppen verwandt.

Der Kunde hat i.d.R. für den Zugang zu Daten bzw. die Rechte zu deren Nutzung bezahlt und hat Anspruch auf hochwertige, vor allem aber korrekte Daten. Nutzung bzw. Weiterverarbeitung nicht korrekter Daten und Leerläufe durch Lieferengpässe, wie sie z.B. durch Ausfälle auf Seiten des Service Providers entstehen können, führen zu falschen oder gar keinen Analysen, die für den Kunden Fehlinformation und/oder Nutzungsausfall bedeuten.
Was beim Privatkunden vielleicht nur Zeitverlust und Ärgernis hervorruft, kann für den Geschäftskunden finanzielle Verluste zur Folge haben.

Der Schutz des Kunden, wie er beispielsweise durch Kryptographie realisierbar wäre, ist in der Praxis aus mehreren Gründen nur schwer zu erreichen. Die Vielzahl der möglichen Schnittstellen und beteiligten Infrastrukturen ist eines der größten Probleme, da es bekannterweise meist schwierig ist, alle beteiligten Partner auf einen Standard „einzuschwören“. Genau dies wäre aber ein guter Ansatz, um Authentizität und Sicherheit der Daten auf ihrem Weg mit Hilfe kryptographischer Methoden zu gewährleisten.

Die Zuordnung einer an einem GIS beteiligten Partei zu einer der drei erwähnten Instanzen ist in der Realität manchmal schwierig, da die Grenzen fließend sind. So kann eine Partei die Rolle mehrerer Instanzen übernehmen, indem sie beispielweise Content und Service Provider darstellt, oder aber auch dadurch, dass sie Inhalte sowie Technik einkauft und Dritten die Nutzung eines GISs anbietet, gar keiner Instanz zuordbar sein.

6 Reales Szenario

Im vorherigen Kapitel wurde gezeigt, dass Gefahrenpotential vorhanden ist. Aus jeder der drei genannten Sichtweisen betrachtet sind Situationen möglich, die einer oder mehreren Instanzen schaden könnten. Diese Schäden treten zumindest mittelbar als finanzielle Verluste in Erscheinung.
Es wurde ebenfalls erläutert, dass Motivationspotential für die Herbeiführung eben dieser Situationen vorhanden ist. Neben den erwähnten Gründen, sich selbst zu bereichern oder Konkurrenten zu schaden, gibt es noch eine Vielzahl weiterer, von denen hier nur die typische Hackermotivation „*ist es möglich?*“ erwähnt sein soll.

Nun stellt sich die Frage, ob es tatsächlich möglich ist, den Willen in die Realität umzusetzen und eine für eine Instanz schadhafte Situation herbeizuführen. Diese Frage soll anhand eines realen Szenarios exemplarisch beantwortet werden.

6.1 Location Based Services

Das Szenario wurde aus dem Bereich der Location / Situation Based Services ausgewählt. Hierbei handelt es sich i.d.R. um Dienste, die mobilen Clients angeboten werden und die direkten Bezug auf dessen aktuelle Position bzw. Situation nehmen. Diese Auswahl wurde aus mehreren Gründen getroffen.

1. Es sollte ein Szenario gewählt werden, bei dem der Datentransfer durch einen ungeschützten Bereich erfolgt, d.h., mindestens ein Teil der Kommunikationsstrecke liegt weder im Einflußbereich des Anbieters, noch in dem des Nutzers. Solch ein Szenario hat den „Vorteil“, dass die Daten während des Transfers zumindest theoretisch angreifbar sind, dies ist bei mobilen Clients, die meist Funknetze nutzen, der Fall.

2. Das Szenario sollte realitätsnah und vor allem zukunftsträchtig gewählt werden. LBS/SBS sind bereits verfügbar und werden genutzt. Weiterhin wird ihnen große Bedeutung in der Zukunft zugesprochen.

6.2 Einführung in TMC/RDS

Das gewählte Zielsystem, das angegriffen werden soll, ist ein in ein KFZ eingebautes Navigationssystem. Dass ein solches System als GIS zu betrachten ist, wurde bereits

in Abschnitt 4.1 ab Seite 18 gezeigt, deshalb sei hier nur daran erinnert, dass es eine Kombination aus Routing-Anwendung und GPS ist.
Den für Normalverbraucher verfügbaren Stand der Technik stellen Navigationssysteme dar, die sogenanntes Dynamisches Routing unterstützen. Hierbei wird das Navigationssystem in Echtzeit mit Verkehrs- und Wetterinformationen versorgt, welche es in die Routenplanung mit einbezieht und so beispielsweise Staus ausweichen kann.
Die Übermittlung dieser Informationen erfolgt über TMC/RDS, welches in [14819/1-6] ratifiziert ist und eine Anwendung des Radio Data Systems darstellt. RDS steht für die Übermittlung digitaler Daten mittels Radiowellen, wie sie von normalen Radiosendern ausgestrahlt werden und wird z.B. auch für die Übermittlung von Sendernamen oder Programminformationen genutzt, die im Display des Radios angezeigt werden können.
TMC steht für Traffic Message Channel und definiert, wie Traffic and Traveller Information (TTI) kodiert werden. Kodierung darf an dieser Stelle nicht im kryptographischen, sonder muß im Datenverarbeitungstechnischen Sinne verstanden werden.
Die Übermittlung von TMC über Mobilfunknetze ist ebenfalls möglich und wird zukünftig wahrscheinlich große Bedeutung haben. Noch ist die Standardisierung in [14821/1-8] aber weder abgeschlossen noch ratifiziert.

Abbildung 6: Schema TMC/RDS

TMC/RDS hingegen ist standardisiert und bereits in großen Teilen Europas verfügbar, wie aus Abbildung 7 ersichtlich ist, und kann von modernen Navigationssystemen genutzt werden.

Abbildung 7: Verfügbarkeit TMC/RDS, Quelle: [tmc-service]

Die bei Verkehrsrechenzentralen eingehenden Meldungen werden an Radiostationen weitergeleitet und über RDS zusammen mit deren FM-Signalen ausgestrahlt. Es dauert typischerweise 30 Sekunden von der ersten Meldung eines Staus, bis die Information im Fahrzeug verfügbar ist. Das Navigationssystem filtert zunächst diejenigen Meldungen heraus, die für die momentane Route relevant sind. Daran schließt sich ein komplexer Prozess an, in dem die Entscheidung darüber getroffen wird, ob eine andere Route gewählt werden soll. Der gesamte Prozess kann je nach Wunsch des Benutzers interaktiv

oder automatisch im Hintergrund ablaufen (vgl. [tmc-what]).
Über TMC/RDS werden neben den derzeit hauptsächlich öffentlichen Gratisdiensten auch Zusatzdienste von kommerziellen Anbietern ausgestrahlt. Das Wort kommerziell lässt bereits vermuten, daß diese Dienste nur für einen eingeschränkten Benutzerkreis, nämlich zahlende Kundschaft, zugänglich sein sollen, was durch kryptographische Methoden, wie in [14819/6] beschrieben, realisiert werden soll.

6.3 Technische Einschränkungen der Kryptographie

Bei der Auswahl bzw. Entwicklung der kryptographischen Algorithmen und Protokolle für die verschlüsselte Datenübertragung über TMC/RDS mussten einige technische Einschränkungen, die durch die beteiligten Systeme vorgegeben sind, berücksichtig werden. Auf Grund der geringen Datenübertragungsrate von RDS musste, um die einwandfreie Funktion des Systems sicherzustellen, darauf geachtet werden, dass das Datenvolumen durch den Einsatz von Kryptographie nicht allzu sehr zunimmt. Somit ist nur wenig Spielraum für kryptographische Methoden vorhanden.
Die geringe Rechenleistung der Endgeräte schloss den Einsatz von rechenintensiven asymmetrischen und sogar aufwendigen symmetrischen Algorithmen zur Verschlüsselung von vornherein aus. Die in [14819/6] definierten Algorithmen bieten nur einfachste symmetrische Verschlüsselung, die durch elementare Funktionen auf der Bit-Ebene (Right-Shift, XOR) realisiert ist.
Diese und andere technische Einschränkungen führen dazu, dass die Daten nur durch „weiche“ Verschlüsselung geschützt sind. Weiterer Schutz der Daten wird dadurch erreicht, dass in den Algorithmen geheime Abbildungstabellen verwandt werden, die nur dem Entwicklerteam, der Standardisierungsbehörde, den Diensteanbietern und den Produzenten der Endgeräte bekannt sind. Die Stärke eines kryptographischen Algorithmus sollte nicht auf der Geheimhaltung seiner Bestandteile beruhen, wie schon in Einführungswerken der Fachliteratur nachzulesen ist. Sollte der Inhalt der Tabellen z.B. durch reverse oder social engineering bekannt werden, wäre der durch sie erreichte Schutz nichtig. Ein neuer Algorithmus, beispielsweise mit veränderten Tabellen, müsste entwickelt und verbreitet werden. Dies würde im Klartext bedeuten, dass die Software in jedem Navigationssystem aktualisiert werden müsste.
Die Entwicklergemeinschaft selbst stellt klar, dass die Verschlüsselung hauptsächlich zur Durchsetzung verschiedener Geschäftsmodelle dient. Der eingesetzte Algorithmus bietet keinen ernsthaften kryptographischen Schutz, sondern ist ausreichend, um die Daten vor

dem Zugriff durch Laien zu schützen. In der zu ratifizierenden Vorlage [14819/6] heisst es hierzu in einem Kommentar:

> „The encryption is only leight but was adjudged to be adequate to deter other than the most determined hacker“.

6.4 Schwachstellen

Eine generelle Schwachstelle von TMC/RDS, die sowohl öffentliche als auch zugangsgeschütze Dienste betrifft, beruht darauf, dass die Empfangsgeräte automatisch den jeweils stärksten Sender auswählen. Dies geschieht, um den einwandfreien Datenempfang auch ohne Benutzereingriffe sicherzustellen und macht die Nutzung eines solchen Systems komfortabel.
Die automatische Senderauswahl stellt aber auch ein Sicherheitsrisiko dar, denn es ist mit verhältnismäßig geringem Aufwand möglich, dem System gegenüber als stärkster Sender aufzutreten und ihm falsche TMC-Daten einzuspielen. So könnte man einem Fahrzeug beispielsweise mit einem anderen Fahrzeug, das mit einem entsprechenden Sender ausgestattet ist, folgen und so die beste Empfangsqualität bieten. Das Erzeugen standardgerechter TMC-Meldungen mit gewünschtem Inhalt ist für technisch versierte Personen unproblematisch, da die Kodierungsstandards öffentlich zugänglich sind. Das angegriffene Zielsystem wird die ausgestrahlten Falschmeldungen empfangen, weiterverarbeiten und ihrem Inhalt entsprechend reagieren.

Doch stellt dies eine wirkliche Bedrohung dar?

6.5 Angriff und Folgen

Im vorigen Abschnitt wurde gezeigt, dass der Angriff auf ein Zielsystem durch Einspielen falscher TMC-Meldungen technisch möglich ist. Dies würde im Extremfall bedeuten, dass der Angreifer die Kontrolle über das Navigationssystem erlangen und beliebige Routenänderungen durch gezielte Falschmeldungen herbeiführen kann.
Für den Benutzer würde dies i.d.R. Zeitverlust und Ärgernis, jedoch keine ernsthaften Schäden, wie etwa finanzielle Verluste, bedeuten.
Wo liegt also der Anreiz, solche Angriffe nicht nur zum Spaß durchzuführen?
Um die Antwort auf diese Frage zu finden, muß man sich den Angriff lediglich in einem etwas größeren Maßstab vorstellen. Was würde wohl passieren, wenn man diesen Angriff

über mehrere Wochen hinweg permanent gegen Systeme eines bestimmten Herstellers ausführen würde? Jeder einzelne Kunde wäre zurecht von der Leistung des Systems enttäuscht und würde eine Werkstatt aufsuchen, um sein Gerät prüfen und reparieren zulassen - ohne Erfolg. Die gebündelte Unzufriedenheit der Kunden könnte zu großen Imageschäden auf Seiten des Produzenten bzw. Anbieters des Systems führen. Es ist also praktisch möglich, gezielt die Systeme eines bestimmten Fahrzeugherstellers anzugreifen und diesen mit dem drohenden Imageschaden zu erpressen.

7 Fazit

GISe stellen die Schlüsseltechnologie des 21. Jahrhunderts dar. Es wurde gezeigt, dass die Einsatzgebiete für raumbezogene Anwendungen extrem breit gefächert sind und dass GISe als mächtige, wie ebenso elegante Analyse- und Visualisierungswerkzeuge einen enormen Informationsgewinn, selbst aus alten Datenbeständen, ermöglichen.

Im Verlauf der Arbeit wurden Gefahrenpotentiale identifiziert und erläutert sowie darauf hingewiesen, dass finanzielle und politische Interessen generell als Motivation für betrügerisches Handeln und Ausnutzung von Schwächen eines Gegners zu sehen sind.

Anhand eines konkreten Beispiels konnte (zumindest) exemplarisch gezeigt werden, dass die neue Technologie Sicherheitslücken, die teilweise erst durch neue Sichtweisen erkennbar werden, mit sich bringt, die Ansatzpunkte für Angriffe bieten.

GISe werden, wie in Abschnitt 4.5 ab Seite 21 nachzulesen ist, auch in Kritischen Infrastrukturen eingesetzt. Dass diese Infrastrukturen besonders schützenswert sind, da Ausfälle und Störungen besonders nachhaltige und weitreichende Folgen haben, wurde in Abschnitt 2.2.3 angesprochen und wird in [BSI] detailliert erläutert. Um das Gefahrenpotential abzuschätzen, dass von Störungen in den beteiligten GISen für die Kritischen Infrastrukturen ausgeht, muss man zunächst für jede Anwendung ermitteln, in wie weit sie unmittelbar von der Funktion des GISs abhängt.
Energieversorger und Telekommunikationsunternehmen beispielsweise setzen GISe hauptsächlich zur Netzplanung und Verwaltung ein, so dass kurzfristige Systemausfälle keinen Einfluss auf die Energieversorgung und Telekommunikationsinfrastrukturen hätten.
Andere kritische Infrastrukturen sind direkt von den eingesetzten GISen abhängig und würden durch Störungen nahezu in Echtzeit äußerst empfindlich in ihrer Funktion beeinflusst. Zu dieser Kategorie zählen z.B. Transport- und Verkehrswesen sowie Notfall- und Rettungsdienste.

Die Folgen von Systemausfällen bei der Flugsicherung am Frankfurter Flughafen oder bei großen Logistikunternehmen sind nur schwer vorstellbar, würden aber mit Sicherheit unverzögert einsetzen. Denkt man über Ausfälle in Zeitfenstern von mehreren Stunden oder Tagen nach, wird klar, warum der Schutz Kritischer Infrastrukturen und somit auch der beteiligten GISe so wichtig ist.

Es besteht akuter Handlungsbedarf, denn Sicherheit in Geoinformationssystemen ist ein wichtiger Themenkomplex, dem bisher viel zu wenig Aufmerksamkeit gewidmet wurde. Da Gefahrenpotenziale, Sicherheitslücken und Gründe, diese auszunutzen, vorhanden sind, müssen GISe, die zukünftig noch an Einfluss gewinnen werden, durch umfassende Sicherheitskonzepte geschützt werden. Dass sich die Risiken dadurch effektiv einschränken lassen, wurde in Kapitel 5 angesprochen, ist unter [BSI2] genauer erörtert und auch aus der Erfahrung mit anderer IT allgemein bekannt.

Literatur

[14819/1-6] CEN/ISO: TTI messages via traffic message coding ISO FDIS 14819 [1-6], http://www.itsa.org/committe.nsf/58900774a054390685 256429006699a7/381c3d0929a87abd85256ba30066b8c1? OpenDocument

[14821/1-8] CEN/ISO: TTI messages via cellular networks prCEN/TS 14821 [1-8], http://www.cenorm.be/standardization/tech_bodies/ cen_bp/workpro/tc278.htm

[14819/6] CEN/ISO: Encryption and condition access for the Radio Data System TMC RDS-TMC ALERT C coding prEN/ISO 14819-6, http://www.itsa.org/committe.nsf/58900774a05439068 5256429006699a7/fe6e6bf6db0e06cd85256ba300739607? OpenDocument

[Bill91] Bill, R. und D. Fritsch (1991): Grundlagen der Geoinformationssysteme. Bd. 1 Hardware, Software und Daten, Heidelberg, Wichmann-Verlag

[Bley02] Große Bley, Andre (2002): Wireless LAN Sicherheit, http://www.etdv.ruhr-uni-bochum.de/dv/lehre/seminar/wlan-sicherheit/wlan-sicherheit-slides.pdf

[Borrough86] Burrough, P.A. (1986):Principles of Geographical Information Systems for Land Ressources Assessment, Oxford, Clarendon Press

[Brockhaus98] F.A. Brockhaus GmbH und Deutscher Taschenbuch Verlag GmbH & Co.KG (1998): Brockhaus Lexikon, Mannheim/München

[BSI] Bundesamt für Sicherheit in der Informationstechnik: Kritische Infrastrukturen, http://www.bsi.de/kritis/kritis.htm

[BSI2] Bundesamt für Sicherheit in der Informationstechnik: Kurzinformation zu IT-Grundschutz, http://www.bsi.de/literat/faltbl/itgrund.htm

[BSI3] Bundesamt für Sicherheit in der Informationstechnik, Sicherheit im Internet, http://www.bsi.de/literat/sinet.htm

[Daratech00] Daratech Inc., (2000)

[EU-Studie00] Commercial exploitation of Europe's public sector information - Pira International Ltd., Universitiy of East Anglia und KnowledgeView Ltd., European Commission, Sept. 2000

[Fecht] Fecht et al.: GIS oder wie beschreibe ich räumliche Phänomene, http://www.fbw.hs-bremen.de/~pschmidt/Material/GIS-Referat.ppt

[Flyer] Deutscher Verein für Vermessungswesen: GIS-Flyer Land/Bund, http://gis.geo.fhm.edu/dvw_ak3/gis-flyer/gis-flyer-land-land.html

[GoogleInc] Google inc.: http://www.google.de/intl/de/profile.html

[HH02] Freie und Hansestadt Hamburg, Wirtschaftsbehörde Strom- und Hafenbau: Europas modernster Containerterminal, http://www.hamburg.de/WiHaVe/Hafen/CTA/

[HHLA] Hamburger Hafen- und Lagerhaus AG, CTA, http://www.hhla.de/C/cont.htm

[Hartmann02] Dr. Söhnke Hartmann (2002), Container-Terminal Altenwerder: Simulation der Logistik, http://www.bwl.uni-hildesheim.de/aglogistik/vortrag-schweinfurt/hartmann.pdf

[Linder99] Linder, Wilfried (1999): Geo-informations-systeme, Heidelberg, Springer-Verlag

[MICUS03] Der Markt für Geoinformationen: Potenziale für Beschäftigung, Innovation und Wertschöpfung - MICUS Management Consulting GmbH, Bundesministerium für Wirtschaft und Arbeit, Januar 2003

[Muhar92] Muhar, A. (1992): EDV-Anwendungen in Landschaftsplanung und Freiraumgestaltung, Stuttgart, Ulmer

[repasAEG] repas AEG: RESY-PAN: Programmsystem für Aufgaben der Netzplanung, http.//www.repas-aeg.de/deutsch/Aktuelles/Presseservice/Pressemitteilungen/Archiv/prn20000817b.htm

[Schmidt02] Schmidt, Jutta und Schmidt, Peter (2002): Business Mapping; in: Dey und Grauvogel: Praxishandbuch - Wirtschaftswissen von A-Z für die erfolgreiche Betriebspraxis, Kissing

[Schü-Ha] Dr.-Ing. Holger Schütt, Dr. Sönke Hartmann: Simulation in Planung, Realisierung und Betrieb am Beispiel des Container-Terminals Altenwerder, http://halfrant.bwl.uni-kiel.de/bwlinstitute/Prod/mab/hartmann/asim2000cta.pdf

[tmc-service] TMC Forum, http://www.tmcforum.com/tmc/services.htm

[tmc-what] TMC Forum, http://www.tmcforum.com/tmc/what_is.htm