Datenschutzverletzungen bei Internetzugängen via Satellit

André Adelsbach und Ulrich Greveler
Horst-Görtz-Institut für IT-Sicherheit, Lehrstuhl für Netz- und Datensicherheit
Ruhr-Universität, 44780 Bochum
www.nds.rub.de

1 Einführung

Viele geostationäre Satelliten sind mit digitaler Funktechnik ausgestattet und können neben Fernseh- und Rundfunkprogrammen auch Daten breitbandig übertragen. Insbesondere für strukturschwachen Regionen, wo es keinen schnellen Zugang (DSL) zum Internet gibt, stellt der satellitengestützte Zugang ein interessantes Angebot für Privatanwender dar. Der PC des Teilnehmers muss dazu über eine DVB-Karte und eine Verbindung zu einer herkömmlichen Satellitenschüssel mit Digital-LNB verfügen. Dann können Internet-Verbindungen über eine Wählleitung hergestellt werden, für die ein breitbandiger Rückkanal über Satellit bereitgestellt wird. Der Durchsatz für den Rückkanal via Satellit beträgt in der Theorie bis zu 40MB/s, ist allerdings für niedrigpreisige Angebote für Privatanwender i. a. auf Durchsatzraten, die auch im DSL-Bereich verfügbar sind, gedrosselt (z. B. 768 kB/s). Auf diese Weise kann eine Vielzahl von Usern den Dienst auf derselben Frequenz nutzen.

Der *Downlink* einer Satellitenverbindung (das sind die Funksignale, die der Satellit absendet) kann grundsätzlich von jeder Sat.-Schüssel in der Ausleuchtzone empfangen werden, nicht nur vom beabsichtigten Empfänger. Dazu muss die DVB-Karte im PC lediglich auf einen Daten-Transponder eingestellt werden und in einen entsprechenden Modus versetzt werden; dann werden alle Daten-Pakete empfangen - auch wenn diese nicht für den Empfänger bestimmt sind. Software-Werkzeuge zur Gewinnung von Datenmitschnitten und deren Auswertung sind frei verfügbar im Internet zu finden. Aus technischen Gründen ist es nicht möglich, festzustellen, ob Daten abgehört werden, da diese von jeder Sat.-Schüssel aufgefangen werden und es keinen Rückkanal gibt, der es dem Sender ermöglicht zu überprüfen, ob und durch wen die Daten empfangen wurden.

Aufgrund dieser Eigenschaften von Satelliten-Verbindungen spielen Sicherheitseigenschaften eine bedeutende Rolle, insbesondere Verschlüsselung ist als Schutz vor Abhören der Verbindung unumgänglich. Unsere Untersuchungen haben jedoch gezeigt, dass es eine hohe Zahl von unverschlüsselten Datenverbindungen von privaten wie kommerziellen Anwendern gibt und dass diese teilweise hoch vertrauliche Daten enthalten [NT04, AG05]. Eine bessere Aufklärung über die Risiken von Internet-via-Satellit-Anbindungen ist daher unumgänglich.

Anbieter von Internet-via-Satellit-Zugangsdiensten

Kunden in Deutschland können aus einer Vielzahl von europäischen Anbietern (Satelliten-Internet-Service-Provider, kurz Sat.-ISP) auswählen, hier eine Auswahl, die keinen Anspruch auf Vollständigkeit erhebt:

- Telekom / T-Online: „T-DSL via Satellit“ (Downlink: 1024 kBit/s)
- Strato: „SkyDSL“ (Downlink: bis zu 4000 kBit/s)
- Filiago: „DSL by Call“ und „Sat-Flat“ (Downlink: bis zu 1536 kBit/s)
- Netsystem: „ADSL via Sat“ (Downlink: bis zu 300 kBit/s)

Die angebotenen Verträge sind Abbonements, Flatrates und Pay-per-Call-Zugänge, so dass den Kunden eine ähnliche Auswahl wie bei herkömmlichen Internetzugängen geboten wird. Die Preise sind im wesentlichen abhängig von Übertragungsmenge und Durchsatzrate. Um einen Zugang nutzen zu können, muss der PC neben der Modem-/ ISDN-Verbindung eine Empfangsschnittstelle (DVB-Karte) enthalten, die via Kabel mit einer Satellitenschüssel (mit Digital-LNB) verbunden ist, dabei kann i. a. die Schüssel, die gleichzeitig zum TV-Empfang benutzt wird, Verwendung finden, so dass viele Benutzer lediglich eine DVB-Karte (ca. 100-200€) anschaffen müssen, wenn sie sich für Internet-via-Satellit entscheiden. Da die *letzte Meile* zum Kunden hier eine Luftschnittstelle ist, kann prinzipiell jeder europäische Anbieter ausgewählt werden, eine Beschränkung auf nationale Anbieter besteht nicht.

Wie Infratest zum Jahresende 2004 ermittelte, stieg die Zahl der deutschen Satellitenhaushalte um über eine Million auf insgesamt 15,47 Millionen (+7%) an. Via Satellit werden somit fast die Hälfte (43%) der deutschen Haushalte versorgt. Datendienste via Satellit können daher einer bedeutenden Zielgruppe angeboten werden.

2 Sicherheits- und Datenschutzproblematik

Ergebnisse von Untersuchungen zu sensitiven Daten im Broadcast-Datenstrom

Unsere Untersuchungen haben deutlich gemacht, dass eine hohe Zahl als hoch-vertraulich einzustufender Daten ungeschützt über den Downlink-Datenstrom abgestrahlt wird [AG05]. So konnten wir anhand eines 24h-Mitschnitts umfangreiche personenbezogene Daten (Name, Adresse, Kartennummer, Einkommen, etc.) von mehreren Personen nachweisen und die E-Mail-Korrespondenz zwischen kommerziellen Nutzern des Internet beobachten (z.B. Angebotsunterlagen militärischer Zulieferer). Dies ist umso erstaunlicher, wenn man berücksichtigt, dass die grundsätzliche Möglichkeit, Broadcast-Daten abzuhören, bereits seit Jahren in der Fachwelt bekannt ist [Dis97] und Absicherungsmöglichkeiten existieren.

Folgen des Fehlverhaltens privater Anwender

Private Internetnutzer, die Satellitenzugänge ungeschützt nutzen, lassen zu, dass die Daten die sie abrufen, in der Ausleuchtzone des Satelliten (Mitteleuropa im Falle von Astra 1E) ausgestrahlt werden. Dies betrifft sowohl private Kommunikation (E-Mail) als auch die Inhalte die bei Nutzung des WWW ausgetauscht werden. Da jeder Nutzer eines ungeschützten Zuganges eine eindeutige Hardwarekennung (die *MAC-Adresse* der DVB-Karte) besitzt, die in jedem ausgestrahlten Datenpaket enthalten ist, können durch den Abhörenden auf einfache Weise Profile erstellt werden, so dass einem Nutzer beispielsweise die abgerufenen Webseiten, die eingegebenen Suchbegriffe bei Suchmaschinen, empfangene Chat-Nachrichten, Transaktionen bei Online-Platform, heruntergeladene Dateien (aus möglicherweise illegalen Quellen), Namen und E-Mail-Adressen seiner Kommunikationspartner etc. automatisiert zugeordnet werden können. Auf diese Weise lassen sich umfangreiche Dossiers über Personen erstellen (siehe Abb. 1)

Zu dieser Datenschutzproblematik kommt noch der Sicherheitsaspekt hinzu, denn durch geschicktes Nutzen von Informationen aus automatisch versandten E-Mails und Browser-Cookies (das sind Steuer-Informationen beim Abrufen von Webseiten) kann ein Angreifer User-Identitäten stehlen, indem er Protokolle zur Änderung von Passwörter ausführt. Die dazu benötigten Informationen können, wie unsere Untersuchungen ergaben, vollständig dem abgehörten Datenstrom entnommen werden. Der Angreifer kann dann ein User-Konto (z. B. für ein Online-Auktionshaus) weiternutzen und in fremden Namen Transaktionen ausführen, während der legitime Besitzer der Identität ausgesperrt wird.

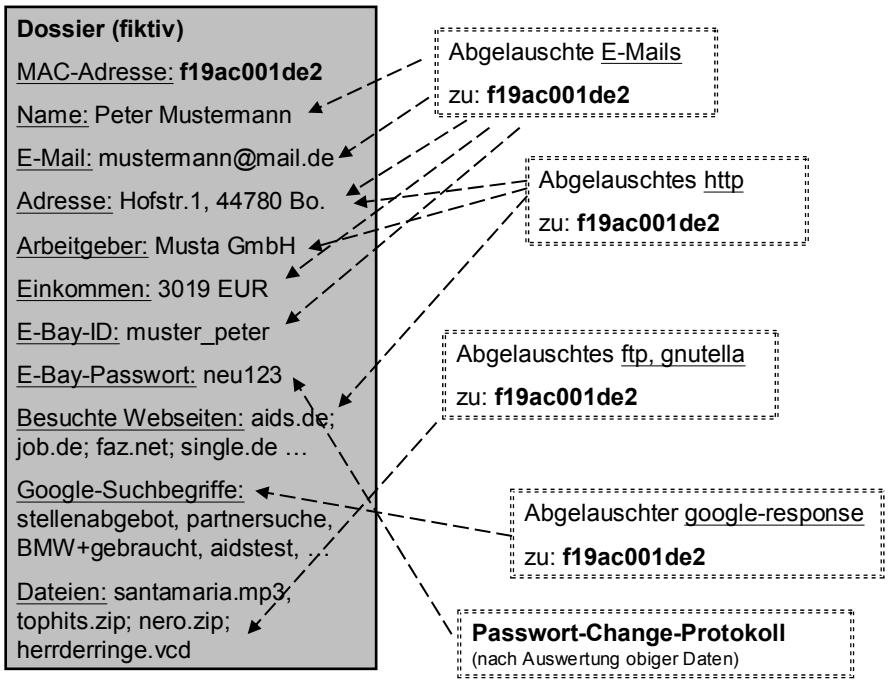

Abb. 1: Zuordnung personenbezogener Daten zu einer Person anhand der MAC-Adresse

Folgen des Fehlverhaltens kommerzieller Anwender

Kommerzielle Internetnutzer, die Satellitenzugänge verwenden, haben ein besonderes Augenmerk auf die Absicherung der Verbindung zu legen, insbesondere wenn sensitive Daten ihrer Kunden übertragen werden. Bei der Untersuchung wurde jedoch festgestellt, dass nicht alle kommerziellen Nutzer dieser Verpflichtung nachkommen. Besonders erschreckend war die Tatsache, dass Onlineshops identifiziert wurden, die ihren Kunden einen sicheren Zugang über das Internet anboten (hier: SSL-Verschlüsselung), aber die vom Kunden übermittelten sensitiven Daten dann über unsichere Kanäle (ungeschützte Satellitenverbindung eines Sat.-ISP) vom Webserver an die interne Buchhaltung weiterleiteten. Wenn solche Daten abgehört werden, liegen die von den Kunden übermittelten personenbezogenen Daten in strukturierter Form vor und können von Unbefugten ohne technischen Aufwand weiterverarbeitet werden.

From: ---------- R LtCol -- SFS/-- [mailto:------@------.af.mil]
Sent: Friday, November 12, 2004 4:06 AM
To: ----------; ------------ F TSgt -- SFS/SF---
Cc: ----------; ----------; ----------; ---------- LtCol
-- SFS/--; ---------- Capt 31 SFS/---; ---------- SMSgt 31 SFS/---
Subject: RE: ---------- System

Mr. ----------,
We would greatly appreciate a sooner installation. We have troops that need this training and can no longer afford to have our system sitting in a warehouse. Let me know if there is anything I can do to help.
Thank you. Lt Col ----------

-----Original Message-----
From: ---------- [mailto:----------.co.uk]
Sent: Friday, November 12, 2004 10:02 AM
To: ---------- TSgt 31 SFS/SF---'
Cc: LtCol 31 SFS/CC'; ------ Capt 31 SFS/---'; ------ SMSgt 31 SFS/---'
Subject: RE: ---------- System

TSgt ----------,
I will contact the Installation and Training team at headquarters in Atlanta USA to see if they can get your system installed sooner.
Regards ----------

(...)
From: ---------- F TSgt 31 SFS/SF---
[mailto:----------@----------.af.mil]
Sent: 12 November 2004 08:43
To: ---------- Cc: ----------; ----------; ----------; ---------- LtCol 31 SFS/--; ---------- Capt 31 SFS/SFT; ---------- SMSgt 31 SFS/---
Subject: RE: ---------- System

All: We would really like to have the -------- set up before then, if you have the resources, please check and see what you can do for our unit. If you can't do it then we would like it done on the first available date that you have. I will be awaiting your response. Thanks for your help in advance.
TSgt ---------- ---------- Training

Abb. 2: abgehörte E-Mail-Konversation von Militärzulieferer
(„-----„ wurde zur Anonymisierung verwendet)

Neben sensiblen Kundendaten werden auf diese Weise zahlreiche interne Firmen-Emails ungeschützt über Satelliten-Internetverbindungen abgerufen (siehe Abb. 2). Unsere Untersuchungen zeigten, dass auf diese Weise Angebotskalkulationen, geheime Produktinformationen und Bewerbungsunterlagen abgerufen und unwissentlich über Mitteleuropa verbreitet werden. Der potentielle wirtschaftliche Schaden lässt sich nur schwer quantifizieren, dürfte jedoch in Einzelfällen mehrere Millionen Euro betragen.

Wie können Verbindungen abgesichert werden?

Prinzipiell existieren mehrere Alternativen zur Absicherung von Satelliten-Internetzugängen. Im Folgenden betrachten wir die möglichen Alternativen und diskutieren deren Vor- und Nachteile.

Absicherung durch dedizierte Proxy-Software

Eine Satelliten-Anbindung hat aufgrund der geostationären Position des Satelliten eine hohe Signallaufzeit-Laufzeit (ca. 0,5s), die eine hohe Latenz bedingt und im Extremfall sogar Unterbrechungen bei Datenverbindungen provozieren kann. Um diese Gesamtlatenz zu verringern bzw. deren Auswirkung auf die Verbindung zu minimieren, bieten viele Satelliten-ISPs eine spezielle Software (engl. *Performance Enhancing Proxy*) an, die neben durchsatzsteigernden Maßnahmen (beispielsweise *Pre-Fetching* von Bildern einer angefragten Webseite oder TCP *Pre-Acknowledgements,* beides technische Maßnahmen zur Beschleunigung der Datenverbindung) auch zur Verschlüsselung des Downlinks verwendet werden kann.

Um die Proxy-Software (und somit deren Sicherheitsfunktionen) zu nutzen, müssen Benutzer ihre Anwendungen (z.B. Web-Browser und Mailanwendung) so konfigurieren, dass diese über die lokale Proxy-Software kommunizieren. Dadurch wird auch eine Absicherung der Daten implizit erzwungen. Die Antworten vom Satelliten-Proxy werden erst vom PC selbst entschlüsselt und an die Anwendung bzw. den Nutzer weitergereicht.

Der Vorteil dieser Lösung ist, dass sich Sicherheit und Durchsatzsteigerung gleichzeitig mit einer Software erzielen lassen, die Nutzer vom Anbieter erhält und ohne technisches Wissen einfach „aktivieren“ kann. Auf der anderen Seite hat diese Lösung auch einige Nachteile. Zum einen wird keine Ende-zu-Ende Sicherheit erreicht, da die Daten nur zwischen Satellit und Endbenutzer verschlüsselt übertragen werden, d. h. in Netzknoten beim Anbieter laufen zunächst alle Daten unverschlüsselt an. Des Weiteren gibt es Konflikte mit etablierten Sicherheitstechnologien wie beispielsweise IPSec, das auf der Netzwerkschicht arbeitet, da der Satelliten-Proxy in das TCP-Protokoll eingreift. Ein weiterer wesentlicher Nachteil besteht darin, dass die Proxy-Software meist proprietäre Sicherheitsmechanismen verwendet und nicht öffentlich spezifiziert ist. Dies verhindert eine Sicherheitsanalyse durch unabhängige Experten, die wesentlich zur Sicherheit offener Sicherheitsstandards wie IPSec oder TLS beigetragen haben. Trotz dieser Nachteile ist diese grundsätzliche Absicherung der Verbindung mittels Proxy-Software immer einer unverschlüsselten Übertragung vorzuziehen, wenn sensitive Daten übertragen werden.

Ende-zu-Ende-Absicherung durch VPN

Eine VPN-Lösung (z. B. Ende-zu-Ende Verschlüsselung und Einbindung des Clients in ein LAN via VPN-Router) kann für einige der Satelliten-Zugänge grundsätzlich eingerichtet werden; leider gibt es dabei jedoch erhebliche Performance-Einbußen, da einige Sat.-Proxy-Technologien (z. B. Pre-Acknowledgements) nicht verwendet werden können. Des Weiteren eignet sich diese Technologie primär dazu die Kommunikation zwischen Rechnern mit Vertrauensbeziehungen, z.B. die Rechner einer logischen Einheit (Unternehmen), zu sichern und zu einem virtuellen lokalen Netzwerk zu verbinden, nicht jedoch, um sicher mit beliebigen Web-Servern zu kommunizieren.

Die VPN-Lösung ist daher nur in Spezialfällen anwendbar, beispielsweise um einen Heimarbeitsplatz sicher über SAT-ISPs in ein Firmennetz einzubinden. Die Kommunikation mit Rechnern außerhalb des Firmennetzes (z.B. Web-Server einer Bank oder eines Online-Auktionshauses) muss durch alternative Maßnahmen gesichert oder unterbunden werden.

Absicherung einzelner Dienste durch den Nutzer

Wenn sich der User auf einzelne Dienste beschränkt und keine weiteren über den Broadcast-Kanal genutzt werden, können diese dediziert (auch von Dritten) auf Anwendungsebene abgesichert werden.

Sicherheitsmaßnahmen auf Anwendungsebene (beispielsweise SSL/TLS beim „Surfen“ im Internet) eignen sich aber auch (alternativ oder komplementär zu VPN-Lösungen) dazu, um Home-Office-Mitarbeitern sicheren Zugang zu Diensten des Firmennetzwerkes zu bieten. In diesem Kontext sind SMTP / POP3 zum Versenden / Abholen der E-Mail und HTTP zum Zugriff auf das Intranet des Arbeitgebers als häufigste Dienste zu nennen, auf die die Kommunikation beschränkt werden könnte.

Gleichzeitig kann jeder Arbeitgeber bei Homeoffice-Arbeitsplätzen Vorsorge treffen, indem er keine unverschlüsselten Zugänge (zum E-Mail-Server oder Intranet) anbietet. So stellt er sicher, dass keine sensiblen Daten über unsichere Kanäle (z.B. ungeschützte Satellitenverbindungen oder WLANs mit schwacher Verschlüsselung) abgerufen werden können, da diese immer verschlüsselt zum Anwender transportiert werden und daher keine Abhängigkeit von sicheren Übertragungswegen gegeben ist.

3 Fazit

Die von uns durchgeführten Untersuchungen haben gezeigt, dass trotz existierender Sicherheitsmaßnahmen personenbezogene und vertrauliche Firmen-interne Daten ungeschützt via Satellit ausgestrahlt werden, da Internet-via-Satellit-Zugänge ohne Absicherung der Daten genutzt werden. Die Ursache dafür ist entweder in der Unkenntnis privater wie kommerzieller Nutzer oder in fahrlässiger Verhaltensweise zu suchen, ungewollte Auswirkungen sind umfangreiche Verletzungen von Persönlichkeits- wie Datenschutzrecht und potentieller wirtschaftlicher Schaden.

Wir sehen die Anbieter der Netzzugänge hier in der Pflicht, ihre Kunden über diese Gefahren aufzuklären. Wir haben gezeigt, dass es technisch möglich ist, festzustellen, welche Nutzer aufgrund fehlerhafter Konfiguration oder leichtsinnigen Verhaltens zu dieser Problematik beitragen und inwieweit personenbezogene Daten übertragen werden; die Anbieter könnten ihrerseits diese Nutzer unter ihren Kunden automatisiert aufspüren und gezielt informieren, da ihnen die Zuordnung von Hardware-Adresse und Kundenkennung schon aufgrund der Vertragsdaten zugänglich ist. Wenn die betroffenen Kunden gezielt über die Folgen ihres Tuns informiert würden, wäre eine Verbesserung der Situation zu erwarten. Insbesondere kommerzielle Nutzer, die Daten ihrer Kunden unwissentlich nicht schützen, haben eine hohe Motivation, diesen Missstand zu beheben, da sie Haftungsansprüche fürchten müssen, wenn sie nach der Aufklärung weiterhin sensitive personenbezogene Daten ungeschützt ausstrahlen.

Literatur

[AG05] André Adelsbach und Ulrich Greveler. *Satellite Communication without Privacy* (Sicherheit 2005, 2. Jahrestagung, Fachbereich Sicherheit d. Gesellschaft für Informatik). Bericht, April 2005.

[Dis97] Dr Dish. *Digital data from the sky*. Zeitschriftenartikel 10/97, TELE-satellite International Magazine, Oktober 1997.

[DB04] Heise News-Ticker (Daniel Bachfeld). *Forscher spähen Satelliten-Internet-Zugänge aus*. Tickermeldung, http://www.heise.de/newsticker/meldung/53676, November 2004.