Getting to know Big Brother

Stefanie Einwang
Betreuer: Matthias Wachs
Seminar Future Internet WS2013/14
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: stefanie.einwang@tum.de

KURZFASSUNG

Es gibt verschiedene Ursachen, warum der Datenverkehr im Internet von verschiedenen Parteien abgehört, manipuliert, verändert oder zensiert wird. Dies geschieht vor allem durch die Filterung von Daten, dem Blockieren von Inhalten oder dem Entfernen von Informationen. Teilweise sind die Ursachen für diese Eingriffe als Hilfe oder Schutz der Bevölkerung anzusehen, bei einigen Gründen spricht dies jedoch eher für die zielgerichtete Beeinflussung der Menschen, um die eigenen Ziele besser zu erreichen. In diesem Paper werden die Gründe und technischen Möglichkeiten erklärt, wie und warum der „Big Brother" auf den Datenverkehr im Internet und auf die Computer zugreift.

Schlüsselworte

Contentfilter, Cookies, Deep Packet Inspection, DNS Manipulation, Firewall, Tracking, Web Bugs

1. EINLEITUNG

Seit den Enthüllungen von Edward Snowden über die Überwachungsprogramme Tempora, Prism und XKeyscore entstehen viele Diskussionen über den Datenschutz und die damit verbundene Überwachung der Bürger. Auch die Politik beschäftigt sich mit dem Thema, jedoch ist noch nicht klar, in welchem Ausmaß E-Mails, Telefongespräche, Chatverläufe oder Ähnliches abgehört und aufgezeichnet werden.

Allerdings kommen immer mehr Fragen auf, die die Internetnutzer zunehmend verunsichern: Wer überwacht den Datenverkehr? Wer wird überwacht? Was wird verändert oder abgehört? Mit welchen Mitteln? Diese Fragestellungen werden im Folgenden beantwortet und geben eine Auskunft darüber, ob der „Big Brother" nur eine Gefahr darstellt, oder möglicherweise auch einen Nutzen mit sich bringt.

So wird im Abschnitt 2 zunächst ein Überblick über den Wandel des Internets von der Entstehung bis heute gegeben, im Abschnitt 3 werden die verschiedenen Interessensgruppen, deren Gründe und Vorgehensweisen dargestellt und abschließend werden im Abschnitt 4 die technischen Grundlagen und Verfahren erläutert.

2. WANDEL DES INTERNETS IM LAUFE DER ZEIT

Zu Beginn der Entwicklungen des Internets war die passive Weiterleitung von IP-Paketen und das Ende-zu-Ende Prinzip die gebräuchliche Architektur. Beim Ende-zu-Ende Argument werden die anwendungsspezifischen Funktionalitäten in den oberen Schichten des Netzwerks implementiert, sodass die unteren Schichten lediglich anwendungsunabhängige Funktionen ausführen, um sämtliche Anwendungen zu unterstützen. Das Internet war dabei ein neutrales Netzwerk, das an zentralen Vermittlungsstellen verwaltet und gesteuert wurde. Die Netzwerkneutralität stellt sicher, dass alle Webseiten und Inhalte gleich behandelt und Anwendungen nicht ausgeschlossen oder bei ihrer Ausführung behindert werden. [5] Es gab keine Einflussnahme auf den Zugang zum Internet und die Informationen, die von den Nutzern konsumiert wurden.

Zwischen 1979 und 1983 wurde das ISO/OSI Schichtenmodell als theoretische Grundlage zur Kommunikation im Internet oder innerhalb von Rechnernetzen entwickelt. Dabei wird zwischen den folgenden sieben Schichten unterschieden, aufsteigend von unten nach oben: Physikalische Schicht, Sicherungsschicht, Vermittlungsschicht, Transportschicht, Sitzungsschicht, Darstellungsschicht und Anwendungsschicht. Jeder Schicht wird dabei vorgegeben, was sie zu tun hat, aber nicht auf welche Weise. Diese strikte Trennung existiert in der Praxis jedoch nicht, da man einerseits die Kommunikationsprotokolle nicht einer bestimmten Schicht zuordnen kann, da dies von der Sichtweise des Betrachters abhängig ist, und andererseits die Trennung der Schichten nicht mit anderen Interessen der Kommunikation übereinstimmen kann. [9]

Auch bei der Implementierung der Funktionalitäten des Internets gibt es heutzutage keine strikte Trennung der anwendungsspezifischen und anwendungsunspezifischen Funktionalitäten mehr. Im Gegensatz zum früher herrschenden Ende-zu-Ende-Prinzip werden jetzt auch anwendungsunspezifische Funktionen in den unteren Schichten implementiert. Dies kann zwar die Ausführung der Anwendungen optimieren, jedoch können die unteren Schichten aber so auch die einzelnen Anwendungen beeinflussen oder blockieren. So kann auch auf die Übermittlung der Daten zugegriffen werden, was zur Überwachung und Manipulation der Inhalte führt. Auf diese Weise geht auch das Prinzip der Netzneutralität verloren, was eine weitere Innovationsfähigkeit des Internets einschränken könnte, da wettbewerbsstärkere Firmen kleinere oder neu entstandene Unternehmen und deren Anwendungen unterdrücken können. [7]

Die Nutzung des Internets ändert sich immer weiter, im Jahr 2012 verwenden rund ein Drittel der Weltbevölkerung das Internet, um Neuigkeiten zu lesen, in Kommunikation zu treten oder ihrer Arbeit nachzugehen. Durch diesen Zuwachs haben vor allem Regierungen das Interesse, die Inhalte zu überprüfen und überwachen oder Zensur zu betreiben, indem Webseiten und deren Informationen gefiltert werden. [12] Dieses Eingreifen in

doi: 10.2313/NET-2014-03-1_07

den Datenverkehr ist länderspezifisch, das bedeutet, dass die Bevölkerung von manchen Ländern Webseiten betrachten und Inhalte veröffentlichen kann, die in anderen blockiert werden.

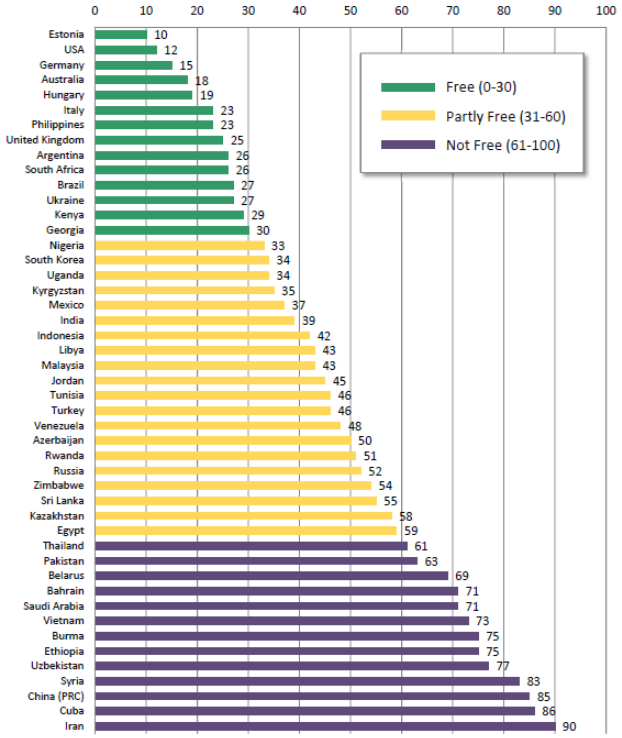

Abbildung 1: Grad der Freiheit im Internet [12], S.21

Der Grad der Internetfreiheit ist in Abbildung 1 dargestellt. Dies wurde in drei Kategorien untersucht, zunächst wie stark die Bevölkerung beim Zugriff auf das Internet oder digitale Medien gehindert wird, zusätzlich inwieweit der Inhalt begrenzt wird und zum Schluss, ob gegen die Benutzerrechte verstoßen wird. [12] Hier ist zu erkennen, dass die Menschen im Iran und in Cuba fast keine Freiheiten haben, im Gegensatz zu Estland und den USA.

Es gibt aber auch weitere andere Manipulationsarten. Das Mit- oder Abhören des Datenverkehrs, das Verändern der übermittelten Daten oder das Unterdrücken der Ausführung bestimmter Anwendungen.

Die technischen Grundlagen für den Einsatz dieser Arten und in welchen Verfahren sie verwendet werden, wird im Folgenden beschrieben. Zunächst wird aber auf die Parteien eingegangen, warum und wie sie diese Vorgehensweisen nutzen.

3. EINFLUSSNEHMENDE INTERESSENSGRUPPEN

Es gibt viele verschiedene Interessensgruppen, die Überwachung und Manipulation des Datenverkehrs veranlassen, um an Daten und Inhalte der Nutzer zu gelangen. Die vier größten Gruppen sind die Politik, Firmen, Webstatistikersteller und Provider, auf deren Motivation und Vorgehensweisen im folgenden Abschnitt genauer eingegangen wird.

3.1 Politik

In Deutschland steht die Politik aktuell im Fokus der Diskussionen bezüglich der Überwachung im Internet und dem dazugehörigen Datenschutz der Bürger. Dazu gehören der von der Regierung finanziell ausgerüstete Bundesnachrichtendienst, die Landeskriminalämter, das Bundeskriminalamt, das Zollkriminalamt, sowie der Militärischer Abschirmdienst. [6]

Der Militärische Abschirmdienst soll die Sicherheit der Bundeswehr gewährleisten. Dazu müssen Informationen gesammelt werden, was einerseits innerhalb der Bundeswehr geschieht und andererseits außerhalb, da auch von hier Gefahren ausgehen können. Dafür bedarf es einer Sicherheitsüberprüfung, um sämtliche Objekte oder Informationen überwachen zu können.

Das Zollkriminalamt ist für die Steuerung von Ermittlungen bei Steuerhinterziehungen, Schmuggeln von Drogen oder anderen illegalen Substanzen und ähnlichen Delikten verantwortlich. Für diese Aufgabe hat das ZKA die Erlaubnis, Informationen zu sammeln, bei Verdacht erfolgt auch eine Online-Überwachung.

Im Inland sind das Bundeskriminalamt und die Landeskriminalämter für den Schutz der Bürger und für die Aufklärung von Straftaten zuständig. Zu diesem Zweck werden Datenbanken geführt, die alle wichtigen Informationen enthalten und die polizeiliche Zusammenarbeit organisieren. Sämtliche mögliche Straftäter oder vermeintliche Vorhaben werden dabei erfasst, was datenschutzrechtlich sehr bedenklich ist. Bei stärkeren Verdachtsmomenten kann außerdem eine Online-Durchsuchung angeordnet werden, um sämtliche Kommunikationsdaten zu analysieren.

Der Bundesnachrichtendienst ist als einziger Geheimdienst für die Auslandsaufklärung zuständig. Ziel des BND ist es, Informationen über das Ausland zu sammeln die für die Sicherheit und die Politik Deutschlands von Bedeutung sind. Dafür wird neben den offenen Quellen wie Zeitungen oder Berichten auch die Telefon- und Internetüberwachung eingesetzt, um an nachrichtendienstlich relevante Informationen zu gelangen. Auf diese Weise können auch internationale Straftaten und Terrorangriffe besser verfolgt und aufgeklärt werden.

Auch der Jugendschutz ist eine Motivation für die Politik, die Inhalte der Webseiten zu überprüfen und gegebenenfalls zu blockieren. Als Vorbild dient hier Großbritannien, die ab Januar 2014 einen sogenannten Pornofilter einführen, der den Zugriff nur bei einer durchgeführten Registrierung erlaubt, die eine Altersbeschränkung von 18 Jahren beinhaltet.

3.2 Firmen

Firmen haben unterschiedliche Anforderungen an das Internet, sodass sowohl die eigenen Produkte gut vermarktet werden können, als auch die Produktivität innerhalb der Firma weiter ansteigt. Ebenso ist die Sicherheit der eigenen Netze eine wichtige Anforderung und soll durch das Eingreifen in den Datenverkehr gewährleistet werden.

Die Motivation lässt sich in zwei große Teile gliedern. Zunächst steht die Sicherheit des eigenen Netzwerks im Vordergrund. Aus diesem Grund werden die Techniken bei den Mitarbeitern eingesetzt. Das private Surfen am Arbeitsplatz soll eingeschränkt werden. Denn dadurch Arbeitsplatz geht die Produktivität zurück, da dem Unternehmen wertvolle Arbeitszeit der Angestellten

verloren geht und die Kapazität der Bandbreite des Internets für produktive Arbeit eingeschränkt ist. Außerdem kann der Mitarbeiter durch private Inhalte Schadsoftware ins Netzwerk einführen, indem E-Mails geöffnet oder Dateien heruntergeladen werden. Auch rechtlich kann das Unternehmen durch das Downloaden von illegalen oder lizenzrechtlich geschützten Inhalten zur Verantwortung gezogen werden. Zudem können vertrauliche Informationen durch die Mitarbeiter nach außen gelangen, was den Konkurrenzunternehmen möglicherweise einen Vorteil verschaffen könnte.

Anhand dieser Probleme, die die Firmen intern lösen müssen werden verschiedene Herangehensweisen eingesetzt. Die häufig zum privaten Surfen verwendeten Webseiten werden mit Hilfe eines Contentfilters gesperrt, sodass keine Zugriffe erfolgen können. Zudem werden sämtliche ein- und ausgehenden Datenpakete über Firewalls überprüft, um einerseits die Sicherheit zu gewährleisten, dass keine Schadsoftware in das Netzwerk gelangen kann, andererseits keine sensiblen Daten nach außen gelangen können. Jedoch werden durch diese Filterungen möglicherweise auch nützliche Inhalte ausgeblendet, wenn sie durch die Firewall oder den Contentfilter blockiert werden, was der Firma wiederum schaden kann.

Als zweiten Ansatz der Motivation lassen sich die Kontrolle des Erfolgs und die Steigerung der Arbeitsleistung und des Produktabsatzes anführen. Hier möchte die Firma das Verhalten ihrer Kunden überwachen, um die Reaktion auf die Einführung neuer Produkte oder Werbemails zu untersuchen. Auch die Kontrolle des Erfolgs ist ein wichtiges Ziel, denn für die Firmen stellt sich die Frage, ob sie ihr Geld wirklich produktiv und effizient investieren. Anhand der Ergebnisse der Analysen des Kundenverhaltens wird die Webseite weiter verbessert und an den Kunden angepasst, sodass der Wert des Unternehmens und damit der Umsatz gesteigert werden.

Dies wird einerseits über Webstatistiken erreicht, die von einem Webstatistikersteller bezogen werden können, oder durch den Einsatz von Cookies oder Web Bugs, die das Nutzerverhalten aufzeichnen und speichern. Diese Datenerhebung ist in § 15 Abs. 3 TMG geregelt: „Der Dienstanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht." [3] Damit kann zielgerichtete Werbung geschalten werden, die anhand des Surfverhaltens auf den Nutzer zugeschnitten ist. Außerdem kann dir Firma nach der Analyse der eingesetzten Web Bugs erkennen, wie der Kunde auf Werbemails reagiert, ob und wann er sie liest, ob er danach auf die Homepage zugreift und diese gegebenenfalls besser auf den Nutzer abstimmen. [12]

3.3 Webstatistikersteller

Der bekannteste Webstatistikersteller in Deutschland ist Google Analytics, was sich auch an der Abbildung 2 erkennen lässt. Google Analytics bietet den Webseiten Betreibern verschiedene Möglichkeiten an, ihre Homepages analysieren zu lassen, beispielsweise die Anzahl und Zeitpunkte der Besuche, den Anteil der wiederholten Besucher der Seite, oder die Benachrichtigungsfunktion bei auffälligen Veränderungen. Dieses Angebot richtet sich an Unternehmen, die ihre Webpräsenz überprüfen und gegebenenfalls durch andere Angebote wie Google AdWords erweitern wollen. [4]

Aber es gibt auch andere Anbieter, die mit der Analyse und dem Sammeln von Nutzerdaten ihr Geld verdienen, zum Beispiel Piwik oder AWStats.

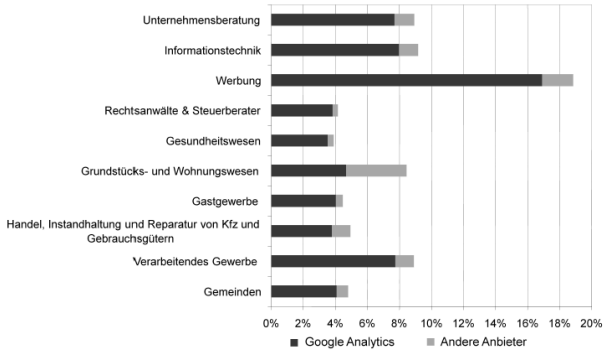

Abbildung 2: Webstatistiknutzer [8]

Anbieter der Webstatistiken machen mit der Analyse von Nutzerdaten ihren Umsatz. Mittlerweile haben sich zudem Informationsallianzen gebildet, über die die Informationen der Nutzer ausgetauscht und weiterverkauft werden. Damit können die umfassenden Wegprotokolle der einzelnen Personen immer weiter und genauer fortgesetzt und anderen Firmen weiterverkauft werden.

Um die Webstatistiken zu erstellen, wird meist mit eigenen erstellten Cookies oder Web Bugs gearbeitet. Hier entscheidet alleine der Dienstleister, welche Daten auf welche Art und Weise gespeichert und analysiert werden.

Eine andere Möglichkeit der Datenerhebung sind Log Dateien. Diese werden vom Betreiber der Webseite erstellt und dann an den Webstatistikersteller weitergegeben, wodurch der Inhaber der Webseite die Kontrolle über die Nutzerdaten hat. [8]

3.4 Provider

Zu den Providern gehören sowohl die Internet- als auch die Mobilfunkbetreiber, die Internetzugänge und Leitungen, sowie Mobilfunknetze zur Nutzung anbieten.

Die Provider haben das Ziel, bestimmte Anwendungen zu sperren, die die Kosten der Nutzung für Dienste des Providers umgehen. Dazu gehören beispielsweise Skype und Voice over IP statt Telefonie oder Instant Messaging statt SMS. Zudem möchten die Anbieter durch Messung der Verkehrsströme herausfinden, an welchen Orten das Netz oder die Leitungen besser ausgebaut werden müssen. Dies geschieht über die Stateful packet Inspection, in der war nicht der Inhalt der Pakete, aber die Art und Menge der Kommunikation überprüft werden kann. [13]

Um die Sicherheit der Computer der Kunden sicherzustellen, werden die ein- und ausgehenden E-Mails und andere ausgetauschte Daten auf Schadsoftware geprüft. Dazu wird die Deep Packet Inspection eingesetzt, allerdings ohne Einsicht von Mitarbeitern, um den Datenschutz der Kunden zu gewährleisten. [13]

doi: 10.2313/NET-2014-03-1_07

4. TECHNISCHE VERFAHREN

Die in 3 aufgezeigten Motivationen der einzelnen Interessensgruppen ziehen eine Reihe technischer Verfahren nach sich, die die Speicherung und die Analyse von Nutzerdaten, die Überwachung von Datenflüssen, oder das Filtern und die Manipulation von Informationen ermöglichen. Diese werden im nächsten Abschnitt genauer erläutert.

4.1 Man-In-The-Middle Angriff

Hauptangriffsziel des Man-In-The-Middle Angriffs ist das Online Banking, aber auch E-Mail Accounts werden ausspioniert. Mit dieser Angriffsmethode werden besonders sensible Daten ausspioniert, mit denen Missbrauch betrieben werden kann.

Bei einem Man-In-The-Middle Angriff dringt der Angreifer in eine Verbindung zwischen zwei Kommunikationspartnern und kann die ausgetauschten Daten in Echtzeit einsehen oder sogar manipulieren. Beide Parteien sehen nicht, dass sie unfreiwillig mit dem dazwischen sitzendem Angreifer kommunizieren, statt ihrem eigentlich erwarteten Kommunikationspartner. Mit diesem Angriff kann auch eine verschlüsselte Verbindung durch Angreifer entschlüsselt und eingesehen werden. [1]

Physikalisch kann dies durch einen direkten Zugriff auf die Leitungen erfolgen, über die der Datenverkehr ausgetauscht wird. In einem WLAN Netzwerk wird meist Snarfing eingesetzt. Die Geräte im Netzwerk werden aufgespürt und im Falle einer Sicherheitslücke wird diese zum Angriff verwendet. Da private WLAN Netze meist verschlüsselt sind, ist die Gefahr in unverschlüsselten öffentlichen WLAN Hotspots deutlich höher. Hier kann auch ein WLAN-Access Point durch einen Hacker nachgeahmt werden, der eine bessere Signalqualität als der original Access Point aufweist. Meldet sich ein mobiles Endgerät an seinem Access Point an, leitet er die Daten zwar zum eigentlichen Access Point weiter, kann aber den gesamten Datenverkehr mitverfolgen. Der Nutzer bekommt von diesem Vorgang nichts mit und kann wie gewohnt im Netz surfen.

Eine Angriffstechnik im lokalen Netz ist das ARP-Spoofing. Dabei werden gefälschte ARP-Pakete zu den Hosts geschickt. Dadurch werden die ARP-Tabellen im Netzwerk so verändert, dass der Datenverkehr dann überwacht werden kann. Um dies zu erreichen müssen beide Hosts, deren Kommunikation überwacht wird, ihre Pakete an den Angreifer schicken. Deshalb sendet er an Host 1 das manipulierte ARP-Paket mit der eigenen MAC-Adresse, statt der von Host 2, und an Host 2 die Nachricht, in der ebenfalls die MAC-Adresse vom Angreifer eingetragen ist. Somit schicken beide Hosts ihre Pakete an den Hacker weiter, der sich damit in der Mitte der Kommunikation befindet.

Eine andere Möglichkeit sind DHCP basierende Angriffe. Dabei simuliert der Angreifer den DHCP-Server, der die IP-Adressen in einem Netzwerk vergibt. Sendet ein Rechner im Netz eine Anfrage nach einer IP-Adresse, antwortet der vorgespielte DHCP-Server schneller als der echte DHCP-Server. Deshalb wird er und seine falsche angegebene Gateway Adresse von den Clients im Netzwerk akzeptiert. Er bekommt auf diesem Weg alle Anfragen der Clients und kann diese einsehen, verändern und weiterleiten. Die Antworten des Webbrowsers kann er abfangen, wenn er den DNS-Server kontrolliert. Hier gibt er seine eigene MAC-Adresse an, sodass alle Pakete zusätzlich zur eigentlichen Zieladresse auch an ihn adressiert werden. [1]

4.2 Cross-Site Scripting

Ziel des Cross-Site Scripting ist es, durch einen in einen Computer oder Webserver eingeschleusten Schadcode die sensiblen Daten des Nutzers zu erlangen und diesem damit zu durch Missbrauch zu schaden oder mit Hilfe dieser Daten das Nutzungsprofil zu erweitern.

Beim Cross-Site-Scripting, kurz XSS, nutzt ein Angreifer eine Sicherheitslücke einer Webanwendung, um Formulare, Passwörter und Cookies des Nutzers auszuspähen. Damit kann er die Cookies manipulieren, die Sitzung übernehmen und die Daten des Nutzers einsehen, verändern oder entfernen. Einsicht in die Daten bekommt der Angreifer meist durch gezielte Täuschung des Anwenders, indem er ihm ein Formular anzeigt, in das die persönlichen Daten eingetragen werden sollen. Zudem hat er die Möglichkeit, Schadcode auf dem Rechner des Anwenders auszuführen, um weitere Informationen zu erreichen. [2]

Die Hacker verwenden meist JavaScript oder Visual Basic Script um einen manipulierten Link auf einem Webserver einzubauen. Dieser wird dann in einem Cookie gespeichert, sodass er bei jedem Aufruf an den jeweiligen Client mitgeschickt wird. Der Link erscheint dem Browser vertrauenswürdig, da er auf einen seriösen Server verlinkt ist. Klickt der Benutzer diesen Link nun an, wird der Code ausgeführt und der Angreifer hat uneingeschränkten Zugriff auf die Sitzung des Opfers. Dieser Vorgang des Angriffs ist in Abbildung 3 dargestellt. Der rote Pfeil zeigt, dass die Daten an den Angreifer gesendet werden, da das infizierte Cookie den Schadcode ausgeführt hat.

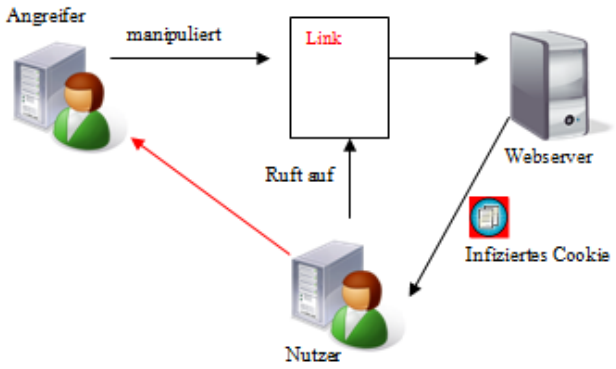

Abbildung 3: Cross-Site-Scripting Angriff

Es gibt drei verschiedene Arten des Cross-Site-Scripting, das persistente, das reflexive und das DOM-basierte XSS.

Beim DOM-basierten Cross-Site-Scripting werden die statischen HTML-Seiten für den Angriff verwendet. Unterstützen sie die Ausführung von JavaScript, wird der Schadcode an das Skript geschickt, das diesen ohne Prüfung ausführt. Für die Durchführung dieses Angriffs wird sowohl ein Skript gebraucht, das Eingabewerte von Daten nicht überprüft, wie auch eine vom Angreifer manipulierte URL, die aufgerufen wird.

Im Gegensatz zum DOM-basierten XSS wird sowohl beim reflexiven als auch beim persistenten Cross-Site-Scripting die Webanwendung auf dem Server miteinbezogen. Beim reflexiven Angriff manipuliert der Hacker die URL und kann damit den dynamischen Teil der Webseite verändern. So kann er den Schadcode temporär in die Webseite einfügen und dann zur Ausführung bringen.

doi: 10.2313/NET-2014-03-1_07

Der Unterschied vom reflexiven zum persistenten Cross-Site-Scripting besteht darin, dass beim persistenten Angriff der Schadcode nicht auf dem Client, sondern auf dem Webserver gespeichert ist und bei jedem Aufruf wieder von neuem ausgeführt wird. Um den Schadcode in der Datenbank des Servers zu platzieren, benutzt der Angreifer Webanwendungen, über die Nutzer Inhalte in die Datenbanken einfügen können. Dazu gehören zum Beispiel Kommentar- oder Gästebuchfunktionen. [14]

4.3 Firewall

Eine Firewall schützt PCs oder Netzwerke vor Angreifern oder schädlichen Inhalten. Dabei können mit bestimmten Filterregeln gezielte Überwachungsmaßnahmen eingeleitet werden, um zum Beispiel die Mitarbeiter einer Firma beim privaten Surfen einzuschränken.

Es wird zwischen der Stateless Firewall, der Stateful Firewall und der Application Level Firewall unterschieden. Je nach Art der Firewall wird die Kommunikation unterschiedlich stark oder schnell geprüft.

Die Stateless Firewall arbeitet auf der Transportschicht und überprüft die Header der ein- und ausgehenden Datenpakete nach bestimmten Filterregeln. Die Filterregeln werden vom Nutzer statisch festgelegt, anhand deren entscheiden wird, wie mit dem Paket umgegangen wird. Dabei werden meist die IP-Adressen von Absender und Empfänger, die Ports, die verwendeten Protokolle und die Netzschnittstellen nach den Kriterien gefiltert. Je nach Ergebnis, wird das Paket dann weitergeleite, verworfen oder an den Absender zurückgeschickt. Das Problem dabei ist aber, dass die Pakete nur isoliert betrachtet werden, das heißt ohne die Informationen über die Filterung der vorgehenden oder nachfolgenden Pakete. Zudem wird der Datenteil der Pakete nicht überprüft. Der Vorteil der Stateless Firewall ist, dass sie sehr schnell arbeitet und einfache Filterregeln beinhaltet, die vom Nutzer bearbeitet werden können.

Die Stateful Firewall betrachtet nicht einzelne Pakete der ein- und ausgehenden Verbindungen, sondern untersucht die Pakete zusammen und prüft zusätzlich den Zustand der Netzwerkverbindung. Dieser unterscheidet sich anhand des verwendeten Protokolls, ist das Protokoll zustandslos, wie http, kann der Zustand nicht analysiert werden. Bei einem zustandsbehafteten Protokoll speichert die Firewall immer wieder Informationen des untersuchten Datenverkehrs und passt damit die Filterregelungen auf den aktuellen Kontext an, sodass die Qualität der Filterung steigt. Dazu gehören beispielsweise die Protokollierung der verwendeten Ports, um Antworten nur am angegebenen Port anzunehmen, oder die Speicherung des Kontextes, sodass erkannt werden kann, ob ein Paket eine Antwort auf ein anderes ist, oder ob die Pakete zusammengehören. Die Stateful Firewall fängt zwar mehr zweifelhafte Inhalte ab, ist aber schwer zu implementieren und bei der Filterung sehr langsam.

Die Application Level Firewall arbeitet auf der Anwendungsschicht und untersucht nicht nur die IP-Adressen, Ports und Netzschnittstellen, sondern auch den Inhalt der Datenpakete. Für jedes Anwendungsprotokoll gibt es für die Filterung einen eigenen Proxy. Dieser baut als neuer Kommunikationspartner eine eigene Verbindung zum Ziel auf, sodass zwei eigenständige Verbindungen entstehen. Dabei werden die Pakete zu einem Datenstrom zusammengefasst und überprüft, anschließend werden sie in neue IP-Pakete verpackt und weitergeleitet. Durch Position als Kommunikationspartner kann er den Kommunikationsfluss beobachten, und auf dieser Basis die Pakete weiter filtern. Diese durchlaufen den gesamten ISO/OSI Stack, sodass zudem der Zustand der Verbindung überwacht werden kann. Die Vorteile der Application Layer Firewall sind also die Überprüfung des Protokolls, die Untersuchung des Inhalts auf Schadsoftware, sowie die Möglichkeit, weitere Dienste wie Virenfilter miteinzubinden. Durch diesen Umfang an Funktionen dauert die Filterung der Datenpakete länger, die Implementierung ist langwieriger als bei der Stateful Firewall und es wird für jedes Anwendungsprotokoll ein eigener Proxy benötigt.

Welche Firewall in welchem System eingesetzt werden sollte, hängt von der erwarteten Leistung der Filterung und dem Sicherheitsniveau ab.

4.4 Deep Packet Inspection (DPI)

Die Deep Packet Inspection ist einerseits für die Sicherheit eines Netzwerks von Bedeutung, da eingehende Datenpakete auf schädlichen Inhalt geprüft werden können, andererseits wird sie dazu verwendet, Inhalte der Nutzer auszuspähen und diese für die eigene Zielerreichung zu verwenden.

Bei der DPI werden sowohl der Header als auch der Datenbereich von Datenpaketen auf unerwünschte Programme oder Anwendungen und Spam überprüft. Dies unterscheidet die DPI von der Stateful Packet Inspection, die lediglich den Header der Pakete untersucht. Bei der Deep Packet Inspection kann der Inhalt des IP-Pakets verworfen oder verändert werden, und die Weiterleitung des ganzen Pakets zeitlich zurückgehalten werden. Sie wird beispielsweise bei Anti-Viren-Software, Contentfiltern oder Firewalls eingesetzt, um Kontrolle über die ein- und ausgehenden Datenpakete zu erhalten.

Für die Nutzung der DPI in Firewalls kann das Pattern Matching oder die Untersuchung der Protokollabweichungen eingesetzt werden. Für das Pattern Matching werden Datenbanken benötigt, in denen bekannte Angriffe auf Netzwerke gespeichert sind. Mit diesen Einträgen der Datenbank werden die Pakete verglichen und bei einem positiven Ergebnis blockiert. Unbekannte Angriffsarten können mit dem Pattern Matching nicht erkannt werden. Bei der Analyse des Pakets auf Protokollabweichungen können auch solche unbekannten Angriffe verhindert werden. Im Gegensatz zum Pattern Matching werden bei diesem Verfahren die erlaubten Verhaltensweisen des Protokolls definiert. Auf Grundlage dieser Festlegungen werden alle erlaubten bekannten Attacken weitergeleitet, unbekannte und nicht erlaubte werden blockiert.

Eine DPI, die Pakete mit Fehlern oder unerwünschten Inhalten in Echtzeit blockieren kann, ist ein Intrusion Prevention System. Diese Fähigkeit wird durch eigene Funktionen des IPS erlangt, indem mit einer Kombination aus Pattern Matching, Stateful Inspection und Anomalieerkennung gearbeitet wird. So wird auch das Netzwerk selbst geschützt, und nicht nur die Angriffe darauf verhindert.

Jedoch gibt es auch einige Nachteile bei der Nutzung der Deep Packet Inspection. Es wird eine eigene Hardware benötigt, die die Ressourcen für die DPI bereitstellt. Zudem müssen regelmäßige Updates durchgeführt werden, um die Software auf dem neuesten Stand des Schutzes zu halten.

doi: 10.2313/NET-2014-03-1_07

4.5 Contentfilter

Der Contentfilter wird meist zur Blockierung unangemessener, anstößiger oder verbotener Inhalte verwendet, sodass die Nutzer des Internets vor diesen Webseiten geschützt werden. In Ländern, in denen Inhalte zensiert werden, wie beispielsweise China oder der Iran, werden diese Contentfilter aber auch dafür verwendet, dass die Webseiten auf Inhalte überprüft werden, die laut der Regierung nicht veröffentlicht werden dürfen.

Der Contentfilter überprüft anhand einer Filterliste den Datenverkehr, um illegale Seiten zu sperren oder anstößige Inhalte auszublenden. Er erleichtert die Kontrolle des Datenaustausches, ohne dass der Nutzer dies merkt. Dies geschieht anhand der eingegebenen Webadresse oder ausgewählter Wörter, Sätze, Bildern und auffälligen E-Mail Anhängen. Die Filterliste wird über regelmäßige Updates durch den Hersteller immer auf dem aktuellsten Stand gehalten.

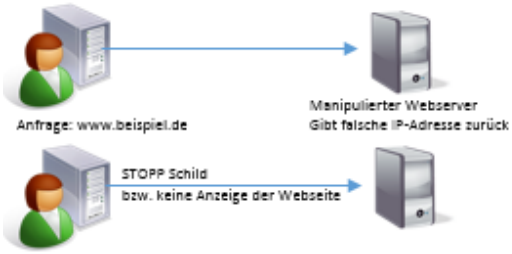

Abbildung 4: DNS-Sperre

Dabei werden verschiedene Verfahren verwendet. Nicht vertrauenswürdige Adressen können in einer Schwarzen Liste gespeichert werden, vertrauenswürdige in einer Weißen Liste. Anhand dieser Schwarzen Liste kann dann die DNS-Sperre eingesetzt werden. Der DNS-Server übersetzt bei einem Aufruf einer Webseite die Webadresse in die zugehörige IP-Adresse. Wenn eine DNS-Sperre im Einsatz ist, wird der DNS-Server manipuliert, sodass er beim Aufruf einer Adresse, die auf der Schwarzen Liste steht, keine IP-Adresse zurückliefert, also keine Verbindung zur Webseite aufbaut. Dieses in Abbildung 4 dargestellte Verfahren kann jedoch leicht umgangen werden. Schwieriger zu umgehen, dafür fehleranfälliger, ist die Sperrung der IP-Adresse. Auch dieses Verfahren funktioniert nur über die Einträge einer Schwarzen Liste. Wird eine eingetragene IP-Adresse aufgerufen, leitet der Router die Daten nicht weiter und blockiert sie. Da aber unter einer IP-Adresse viele Webseiten liegen, werden durch die Sperre auch vertrauenswürdige Seiten blockiert, was zu einer hohen Fehleranfälligkeit führt.

Wenn die Filterung auf Wort- oder Grafikerkennung aufbaut, werden entweder einfache oder intelligente Contentfilter verwendet. Einfache Filter überprüfen das Vorkommen bestimmter Auswahlkriterien. Ist dies mindestens einmal der Fall, wird die Webseite gesperrt. Die künstliche Intelligenz, die der intelligente Filter beinhaltet, untersucht das Vorkommen der Auswahlkriterien zusätzlich nach der Relevanz. Erst wenn ein bestimmter Grad der Überschreitung der Grenzen erreicht wird, blockiert er die Seite. Damit erkennt der intelligente Filter mit einer höheren Wahrscheinlichkeit, ob eine Webseite vertrauenswürdig ist, oder nicht.

Bei der Worterkennung wird der Quellcode des HTML-Dokuments nach bestimmten Wörtern oder Wortfolgen untersucht. Ist ein nicht erlaubter Teil vorhanden, wird der Inhalt gesperrt und ist für den Nutzer nicht mehr sichtbar. Bei der Grafikerkennung reicht diese Untersuchung des Quelltextes nicht aus. Hier werden die Bilder nach bestimmten Farben, Farbkombinationen, Formen und Zusammenhängen gescannt. Verstößt eines dieser Merkmale gegen die Filterregeln, wird die Webseite blockiert. Die heuristischen Verfahren kombinieren die Bild- und Grafikerkennung. Damit wird die Fehlerrate reduziert, das heißt, es werden weniger vertrauenswürdige Webseiten fälschlicherweise gesperrt.

Contentfilter können an verschiedenen Stellen in den Datenverkehr eingreifen, als Software oder Teil des Netzwerks in Proxys, Firewalls oder DLPs. Sie können bereits im Netzwerk eines Betriebs vorhanden sein, sodass alle ein- sowie ausgehenden Informationen der vorhandenen Arbeitsplätze im Netzwerk überprüft und gefiltert werden. Die Einstellungen werden dabei vom Besitzer des Netzwerks vorgenommen. Ein E-Mail-Filter überprüft den Text, Anhänge und Bilder der E-Mail auf unerwünschte Inhalte. Zudem wird untersucht, ob die Absenderadresse auf der Schwarzen Liste steht. Der am einfachsten einzusetzende Filter ist der im Browser integrierte Filter, der Anfragen direkt untersucht und gegebenenfalls sofort blockiert, wie auch die Filter in Suchmaschinen. Aber ein Contentfilter kann auch direkt auf dem Computer installiert sein, um den Datenverkehr auch auf schädliche Software zu überprüfen. Dieser kann durch den Administrator eingestellt und verändert werden.

Jedoch gibt es auch einige Probleme beim Einsatz von Contentfiltern. Die Software kann zu stark oder zu schwach blockieren, was zum Scunthorpe Problem führen kann. Dabei werden Webseiten oder E-Mails blockiert, die eine Zeichenfolge enthalten, die eigentlich in Ordnung ist, aber in einem unangemessenen Wort vorkommt. [10] Zudem gibt es Wörter, die zwei oder mehr Bedeutungen besitzen, und eine davon durch einen Contentfilter erkannt und somit der Inhalt gesperrt wird. Bei einer zu schwachen Blockierleistung werden dem Nutzer Inhalte angezeigt, die eigentlich durch den Filter blockiert hätten werden sollen.

4.6 Cookies und Web Bugs

Bei der Verwendung von Cookies auf Webseiten werden die persönlichen Einstellungen des Nutzers gespeichert, beispielsweise der Nutzername und das Kennwort eines Profils, den Warenkorb in einem Online Shop oder Benutzereinstellungen bei Online Suchdiensten. So kann die Webseite auf den Benutzer angepasst und ein Profil über die Webseitenbesuche angelegt werden. Zunächst wird nur die IP-Adresse des Besuchers gespeichert, gibt dieser aber seine Personalien an, werden diese mit der IP-Adresse verknüpft, sodass daraus ein genaues persönliches Profil entsteht. Dieses Verfahren wird meist von Firmen mit Online Shops oder Webseiten genutzt, die das Nutzungsverhalten der Besucher beobachten oder die Seite besser auf die Bedürfnisse des Kunden anpassen möchten.

Ein Cookie ist eine Datei, die die Lebensdauer, den Namen und den Inhalt als Textwert enthält, der vom Webserver festgelegt wird. Auf diese Wiese werden Informationen im Browser gespeichert, und der Nutzer wird bei einem erneuten Besuch wieder erkannt. Ohne Cookies ist dies nicht möglich, da das im Internet meist verwendete HTTP-Protokoll zustandslos ist. Das bedeutet, dass alle Anfragen als unabhängige, einzelne Transaktionen ausgeführt werden, ohne Informationen über die

doi: 10.2313/NET-2014-03-1_07

Sitzung auszutauschen. Abhilfe dagegen schaffen Cookies, deren Erzeugung und Austausch im Folgenden genauer erklärt wird.

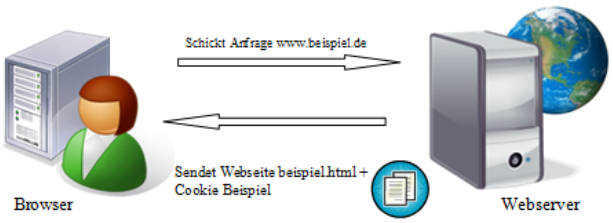

Abbildung 5: Austausch zwischen Browser und Webserver

Wie in Abbildung 5 dargestellt, kann das Cookie zwischen dem Browser und dem Webserver der besuchten Seite ausgetauscht werden. Dabei wird die Eingabe der Webadresse durch den Nutzer als Anfrage an den Webserver geschickt. Dieser beantwortet die Anfrage und sendet den Inhalt der Webseite und die Cookies zurück an den Browser, der im Anschluss die Cookies speichert und die Webseite darstellt. Wird die Seite nun erneut aufgerufen, können über die gespeicherten Cookies die persönlichen Einstellungen des Nutzers wieder aufgerufen und erweitert werden.

Die Web Bugs können im Gegensatz zur den Cookies auch über die Grenzen der einzelnen Webserver hinaus Daten sammeln und zusammenfügen. Damit können die Nutzungsprofile über die gesamte Sitzung erweitert und die Reihenfolge der angeklickten Webseiten gesammelt werden. Es lässt sich zudem erkennen, ob und wann E-Mails gelesen wurden, welcher Browser verwendet wird und welche IP-Adresse der Besucher benutzt. [11]

Web Bugs werden vom Anbieter als transparentes Bild oder Werbung in seine Webseite eingefügt. Hinter diesem Bild versteckt sich ein Link des dritten Servers. Der Benutzer bemerkt nicht, dass seine verwendete IP-Adresse, die URL der besuchten Webseite, die URL des Web Bugs, der Zeitpunkt seines Besuchs, der von ihm benutzt Browser und vorher gesetzte Cookies an den dritten Server geschickt werden, der damit das Bewegungsprofil über die Webservergrenzen hinaus erstellt.

4.7 Registrierungspflicht bei SIM Karten und Internetcafés

Zur besseren Strafverfolgung und Überwachung der Bürger besteht wie in der Schweiz und einigen anderen EU-Ländern auch in Deutschland eine Registrierungspflicht für SIM Karten, sowohl für Prepaid-, als auch für Vertragskarten. Bei Abschluss eines Vertrags sind die persönlichen Daten anzugeben, sodass der Nutzer eindeutig identifiziert werden kann. Bei der Nutzung einer Prepaidkarte muss der Kunde diese nach dem Kauf zunächst freischalten. Dies geschieht, wie auch bei Vertragsabschluss, mit den persönlichen Daten. Ohne diese Freischaltung erfolgt keine Einwahl ins Netz des Mobilfunkbetreibers.

Jedoch wird dieses Gesetz immer wieder umgangen. Einerseits ist durch den Tausch oder die Weitergabe keine Verfolgung der Daten möglich, da hierbei keine Verpflichtung zur erneuten Freischaltung mit den aktuellen Daten besteht, andererseits gibt es im Internet Unternehmen, die anonyme SIM Karten vertreiben.

Auch in Internetcafés wird die Anonymität der Nutzer unterbunden, da die Personalien aufgenommen werden und in der Datenbank des Betreibers des Internetcafés gespeichert werden.

In Deutschland herrscht bis zum heutigen Zeitpunkt allerdings keine Ausweispflicht, was manche Nutzer des kostenpflichtigen Zugangs zum Internet dazu führt, illegale Seiten, Posts, Bilder oder Ähnliches zu suchen und weiterzuverbreiten. Um bei Missbrauch des Internetzugangs jedoch eine Strafverfolgung zu ermöglichen, ist meist Videoüberwachung im Einsatz, um Besucher identifizieren und notwendige Ermittlungen einleiten zu können.

5. ZUSAMMENFASSUNG

Anhand des Papers kann man erkennen, dass es viele technische Möglichkeiten der Überwachung, der Manipulation oder dem Verändern des Datenverkehrs gibt. Diese Verfahren werden auf sämtlichen Ebenen der Kommunikation eingesetzt, von den physikalischen Leitungen durch einen Man-In-The-Middle Angriff bis hin in die oberste Schicht, wo die Cookies im Browser gespeichert werden, der die Anwendung des Nutzers darstellt.

Da die unterschiedlichen Interessensgruppen verschiedene Ziele haben, und aus diesem Grund versuchen, Anwendungen der Konkurrenten in ihrer Ausführung zu behindern schränkt sich die Netzneutralität immer weiter ein. Auch die Motivationen für dieses Eingreifen in den Datenverkehr sind vielfältig, hier liegt der Schwerpunkt vor allem auf der Durchsetzung der eigenen Interessen. Aber auch die Belange der Nutzer werden an manchen Stellen berücksichtigt, beispielsweise bei der Anpassung der Webseiten an die Kunden und deren Bedürfnisse oder beim Schutz der Bevölkerung vor Terrorangriffen oder Straftätern.

Aber die Möglichkeiten der Überwachung des Datenverkehrs und der Modifikation der Inhalte entwickeln sich immer weiter, entweder durch neue Programmiersprachen, oder auch durch die wachsende Zahl mobiler Endgeräte, die durch das mobile Internet oder Hotspots leichter zum Ziel eines Angriffs werden. Viele Nutzer sind mit dem Umgang ihrer Daten auch unvorsichtig, und prüfen nicht, wem sie ihre persönlichen Angaben hinterlassen. Aus diesen Gründen sollten sich die Anwender vor allem mit den Maßnahmen zum Schutz gegen Angriffe vertraut machen, um dem Datendiebstahl selbst entgegenzuwirken.

6. REFERENZEN

[1] A. Aurand, „LAN-Sicherheit", dpunkt.verlag, September 2004

[2] D. Fox, „Cross Site Scripting", Datenschutz und Datensicherheit, 11/2012

[3] Diensteanbieter im Sinne des TMG: Bundesrepublik Deutschland, http://www.gesetze-im-internet.de/tmg/__15.html, aufgerufen am 10.09.2013

[4] Google Analytics, http://www.google.com/analytics/, aufgerufen am 04.09.2013

[5] J. Kruse, "Internet-Überlast, Netzneutralität und Service-Qualität", Wirtschaftsdienst, 03/2008

[6] K. Selchert, http://www.geheimdienste.org/, aufgerufen am 22.10.2013

[7] M. Bärwol, „Netzneutralität: Fünf Fragen und Antworten", 18.01.2011

[8] N. Lepperhoff, B. Petersdorf, „Datenschutz bei Webstatistiken", Datenschutz und Datensicherheit, 04/2008

[9] Prof. Dr.-Ing. G. Carle, “Grundlagen Rechnernetze und verteilte Systeme”, 2013

[10] Professional Security Magazine Online, „The Scunthorpe Problem“, 12.09.2013

[11] R. Grimm, „Spuren im Netz“, Datenschutz und Datensicherheit, 02/2012

[12] S. Kelly, S. Cook, M. Truong, „Freedom on the Net 2012“, Freedom House, September 2012

[13] Telekom AG, http://www.telekom.com/verantwortung/datenschutz/1932, aufgerufen am 22.10.2013

[14] Vulnerability-Lab, „CROSS-SITE-SCRIPTING“, Juli 2011

doi: 10.2313/NET-2014-03-1_07