E-Mail-Mithörer

Niklas Baier, Jonas Hielscher, Rawan Jouli,
Moritz Marquardt

30. Juni 2019

Inhaltsverzeichnis

Diese Arbeit wurde im Rahmen des wissenschaftlichen Seminars IT-Sicherheit an der Otto-von-Guericke-Universität Magdeburg im Juni 2019, unter der Leitung von Prof. Jana Dittmann und Robert Altschaffel angefertigt.

Die Autoren sind die folgenden Bachelorstudenten der Informatikfakultät:

> Moritz Marquardt
> moritz.marquardt@st.ovgu.de

> Jonas Hielscher
> benedikt.hielscher@st.ovgu.de

> Niklas Baier
> niklas.baier@st.ovgu.de

> Rawan Jouli
> rawan.jouli@st.ovgu.de

Otto-von-Guericke-Universität Magdeburg
Universitätsplatz 2
39106 Magdeburg

Abstract

Wir untersuchen die in Deutschland weit verbreitenden E-Mail-Anbieter GMX, T-Online, Outlook und Google Mail auf ihre Datenschutzkonformität. Dazu untersuchen wir den Datenverkehr der jeweiligen Web-Clients, die Einbindung von Drittanbietern und die Datenschutzbestimmungen.

Mithilfe eines selbst erarbeiteten Bewertungsschemas vergleichen wir so das Verhalten der Online-Postfächer dieser Anbieter, sowie den Inhalt derer Datenschutzbestimmungen.

Motivation

Diese Arbeit wurde im Rahmen des Wissenschaftlichen Seminars IT-Sicherheit an der Otto-von-Guericke-Universität, unter der Leitung von Prof. Jana Dittmann und Robert Altschaffel angefertigt.

Bei E-Mail Anbietern laufen alle Informationen von Internetnutzern zusammen. Onlinedienste erfordern eine Anmeldung mit einer E-Mail Adresse und senden später Updates an diese Adressen. Da auch sicherheitskritische Funktionen über E-Mails bereitgestellt werden (z.B. das zurücksetzen von Passwörtern) sollten E-Mail Anbieter besonders hohe Sicherheits- und Datenschutzstandards erfüllen.

Die Sicherheit von E-Mail Anbietern z.B. mit Blick auf die Verschlüsselung, oder dem Schutz vor SPAM Mails[1] wurde schon oft beurteilt. Auch werden Anbieter nach Leistungs- und Sicherheitskriterien direkt miteinader verglichen. Diesen Ansatz verfolgen wir auch mit unserer Arbeit: Wir vergleichen eine Reihe der in Deutschland am häufigsten genutzten E-Mail Anbieter nach Kriterien des Datenschutzes, insbesondere in Bezug auf die Einbindung von Drittanbietern in die Web-Clients der Portale.

Ziel ist es zu überprüfen ob die untersuchten Anbieter sich datenschutzkonform verhalten und zu beurteilen ob auch für nicht IT affine Personen eine Benutzung ohne Datenschutzverletzungen möglich ist.

Jonas Hielscher
benedikt.hielscher@st.ovgu.de

[1] Tariq Banday, “Analyzing Internet E-Mail Date-Spoofing” (Digital Investigation Journal, 2011), https://www.sciencedirect.com/science/article/pii/S1742287610000812#!

E-Mail Anbieter

Google Mail

Gmail

Die Googlemail ist mit über einer Milliarde Nutzern die weltweit meist benutzte Plattform zum Versenden und Empfangen von Emails. Die werbefinanzierte Oberfläche ist seit dem 1. April 2004 verfügbar und zeigt ein ständiges Wachstum. Jedoch ist Gmail in Sachen Datenschutz schon mehr als einmal in das Visier der Datenschützer geraten. https://codeberg.org/ovgu/itsec-email-comparison/src/branch/master/paper/images/Gmail-MailAnbieter.png

Kritik App-Entwickler, die Teil des Gmail-Programms von Google sind, dürfen diese E-Mails unter bestimmten Umständen lesen, um neue Dienste oder App-Funktionen zu erstellen, heißt es. Der Großteil der E-Mails würde automatisch per Computersoftware gescannt, in einigen Fällen sollen aber menschliche Mitarbeiter mitgelesen haben. Return Path, ein Unternehmen, das sich E-Mail-Marketing auf die Fahnen geschrieben hat, hat angeblich die Posteingänge von mehr als 2 Millionen Menschen gescannt und 8000 E-Mails ausspionieren lassen.

Funktionen

Der Zugriff auf die E-Mails erfolgt mit einem E-Mail-Programm über TLS-POP3 und TLS-SMTP; seit Oktober 2007 ist der Abruf via IMAP möglich. Die Ablage empfangener E-Mails erfolgt nicht, wie bisher allgemein üblich, in verschiedenen Ordnern, sondern in einem zentralen Mailarchiv. Ferner werden Nachrichten in Themen, von Google „Konversationen“ genannt, zusammengefasst. An die Stelle von Ordnern treten bei Gmail sogenannte „Labels“, die frei definiert und per Mailfilter oder manuell den Nachrichten zugeteilt werden können. Durch diese Labels ist es möglich, Mails – im Gegensatz zur gewöhnlichen Ordnerstruktur – mehreren Kategorien zuzuordnen. Der wesentliche Unterschied von Gmail zu anderen Freemail-Diensten besteht im Funktionsangebot der browserbasierten Oberfläche, das sich an eigenständigen E-Mail-Programmen (wie zum Beispiel Outlook oder Thunderbird) orientiert. Dieses wurde in großen Teilen mit einer als Ajax bezeichneten Technik in JavaScript sowie DHTML realisiert und umfasst ein Adressbuch, eine Rechtschreibprüfung sowie weitere per Tastenkombination zugängliche Funktionen. Diese sind ähnlich schnell und komfortabel wie ein lokal installiertes Mail-Programm, da die Funktionen größtenteils clientseitig, das heißt auf dem lokalen Rechner, ausgeführt werden.

Außerdem lässt sich die Weboberfläche von Gmail um meist nützliche Funktionen erweitern, indem man neue Funktionen in den Gmail Labs aktiviert. Zudem existiert eine Vielzahl von autorisierten und

nicht-autorisierten Erweiterungen für Gmail. Beispielsweise gibt es Nachrichten-Prüfer zur Anzeige der derzeitigen Anzahl neuer Nachrichten oder Programme wie GmailFS, die Gmail-Konten als virtuelle Laufwerke nutzbar machen. Um die Verwendung von Gmail auch im Offline-Modus zu gewährleisten, benutzte der Dienst seit Anfang 2009 Gears, das im November 2011 eingestellt wurde. Um mehr Nutzer zu erreichen, wird dafür seitdem auf HTML5 gesetzt.

Eine gerade bearbeitete Mail wird von Gmail automatisch zwischengespeichert, sodass bei Verbindungsabbrüchen oder Zeitüberschreitungen nur Teile des geschriebenen Textes verloren gehen können. Auch wird durch eine Sicherheitsabfrage überprüft, ob ein Seitenwechsel vom Benutzer beabsichtigt ist, sofern auf diese Weise ungespeicherter Text verloren gehen würde.

Auf Mobilgeräten wird eine spezielle Benutzeroberfläche angezeigt. Diese umfasst zahlreiche Funktionen der Gmail-Desktop-Oberfläche, aber angepasst auf kleinere Bildschirme.

Sicherheit

Gmail nutzt die neuesten Sicherheitsstandards. Durch Pishing-Angriffe können Hacker mit viel Aufwand jedoch trotz Zwei-Faktor-Authentifizierung Mails abfangen und ein Konto knacken.

Mit seinem neuen Feature „Advanced Protection" schwingt Google sich zum wohl sicheresten Anbieter der Welt auf. Ein USB-Stick für den Computer und ein Bluetooth-Chip für mobile Geräte dienen als Schlüssel. Ohne den Schlüssel ist es für Hacker unmöglich, sich in Ihr Konto einzuloggen. Dieses Feature schafft ein hohes Maß an Sicherheit. Für Privatpersonen sind die Standard-Sicherheitsfeatures von Gmail jedoch vollkommen ausreichend. https://codeberg.org/ovgu/itsec-email-comparison/src/branch/master/paper/images/GmailSicherheit.jpg

Email Versand und Empfang

- Sie schreiben Ihre Mail und klicken auf Senden dann teiltdas E-Mailprogramm die Mail nun in “Header” und “Body” auf. Im “Header” stehen relevante Informationen wie Absender, Empfänger usw., der “Body” enthält den eigentlichen Text.
- Wenn die Mail Sonderzeichen (ä,ö,ß,&…) enthält, werden diese umgewandelt, codiert. - Enthält die Mail einen Anhang (Foto, Video, MP3…) wird auch dieser codiert. Der Virenscanner wird aktiv, prüft den Anhang auf Schädlinge.
- Das E-Mailprogramm nimmt Kontakt zum eigenen Mailserver auf und der Mailserver überprüft, ob die Mail zu groß ist. Ist das der Fall, geht sie mit einer Fehlermeldung an den Absender zurück.
- Der Inhalt der Mail wird vom Mailserver gespeichert und derer eigene Mailserver versucht den Mailserver des Empfängers im Netz ausfindig zu machen.

- Dann endlich geht die Mail auf die Reise. Der eigene Mailserver verschickt die Mail an den nächsten Verteilerknoten. Von da geht es über weitere Knoten zum Mailserver des Empfängers.
  - Kurz vor dem Ziel nimmt die Mail Kontakt zu dem Empfänger-Mailserver auf. Antwortet dieser, ist alles gut. Antwortet er nicht, folgen noch ein paar Versuche. Klappt's dann immer noch nicht, geht die Mail mit Fehlermeldung zurück an den Absender

Verschlüsselte Verbindungen Das Versenden von Emails findet bei Gmail über eine gesicherte und verschlüsselte HTTPS Verbindung statt. Das diese wirklich verschlüsselt ist, erkennt man unter anderem auch an dem "s" im https zu Beginn der URL. Bei der Datenübertragung zwischen Ihnen und den Google Servern sind Ihre Mails somit völlig abhörsicher.

Datenschutzerklärung

- Benutzer kann Inhalte aus bestimmten Google-Diensten löschen.
- In manchen Fällen behalten sie Daten für eine begrenzte Zeit zurück, wenn dies zu legitimen Geschäftszwecken oder aus rechtlichen Gründen nötig ist.
- Google nutzt die von uns im Rahmen ihrer Dienste erhobenen Daten für Breitstellung ihrer Diente.
  https://codeberg.org/ovgu/itsec-email-comparison/src/branch/master/paper/images/GmailDatenschutz.png

Rawan Jouli
rawan.jouli@st.ovgu.de

Outlook

Zahlen und Fakten

Nutzerzahlen Outlook.com hat über 400 Millionen Nutzer[2], und ist in Deutschland mit 9,6% der fünftbeliebteste E-Mail-Provider.[3]

Gründung Der Dienst existiert seit 1995 unter dem Namen “Hotmail”, und wurde kurz darauf von Microsoft übernommen.[4]

Kritik Wie Google auch verwertet Microsoft die Inhalte der E-Mails für weitere Zwecke wie beispielsweise Cortana, im Gegensatz zu Google aber nicht für die Personalisierung von Werbung. Personalisierte Werbung wird bei Outlook dennoch angezeigt, die Daten hieraus stammen jedoch nicht aus den E-Mail-Daten, sondern aus anderen Quellen.[5]

Funktionen

Das kostenlose Konto umfasst 15 GB Speicherplatz[6], über die Business-Verträge ist auch der Support für eigene Domains gegeben.[7] Microsoft wirbt damit, dass E-Mails, Kalender und Dateien miteinander verbunden sind, und so ein einfacherer Workflow möglich ist. Zudem werden E-Mails automatisch nach Kategorien und Relevanzen sortiert.[8]

Sicherheit

Eigene Angaben Es gibt keine besonderen Sicherheitsfunktionen, für die der Anbieter wirbt, aber alle normalen Sicherheitsvorkehrungen werden getroffen. Es existieren zusätzlich weitere Sicherheitsfunktionen wie beispielsweise eine Zwei-Faktor-Authorisierung.

[2] http://winfuture.de/news,75884.html abgerufen am 05.07.2019
[3] https://de.statista.com/statistik/daten/studie/151754/umfrage/nutzeranteile-von-e-mail-anbietern-in-deutschland/ abgerufen am 28.06.2019
[4] http://blogs.office.com/b/microsoft-outlook/archive/2012/07/31/introducing-outlook-com-modern-email-for-the-next-billion-mailboxes.aspx abgerufen am 27.10.2012
[5] https://privacy.microsoft.com/de-DE/privacystatement abgerufen am 05.07.2019
[6] https://support.office.com/de-de/article/Speicherbegrenzungen-in-Outlook-com-7ac99134-69e5-4619-ac0b-2d313bba5e9e abgerufen am 05.07.2019
[7] https://support.office.com/en-us/article/Change-your-email-domain-in-Outlook-com-Premium-cc47f494-8679-4365-97c1-e709aebf727e abgerufen am 05.07.2019
[8] https://outlook.live.com/owa/ abgerufen am 05.07.2019

Unverschlüsselte Verbindungen HSTS wird verwendet, um MITM-Angriffen vorzubeugen, outlook.com ist jedoch nicht in der HSTS-Preload-Liste.[9] Die Seite ist positiverweise nicht per HTTP erreichbar, hier gibt es nur eine Weiterleitung zu HTTPS; der Server erreicht hierbei den Grade A bei den Qualys SSL Labs[10]. E-Mails werden nicht verschlüsselt gespeichert.

Erstellen eines Nutzerkontos

Um ein Nutzerkonto zu erstellen, werden die gewünschte E-Mail-Adresse, ein Passwort, Vor- und Nachname, Land und das Geburtsdatum benötigt. Zusätzlich müssen die Datenschutzbestimmungen akzeptiert werden, wobei viele Tracking-Cookies deaktiviert werden können.

Insgesamt ist ein Konto sehr einfach erstellbar und benötigt keinerlei direkt persönlich identifizierbare Informationen (Telefonnummer, Adresse, …) wie bei vielen anderen Anbietern.

> Moritz Marquardt
> moritz.marquardt@st.ovgu.de

[9] https://hstspreload.org/?domain=outlook.com abgerufen am 05.07.2019
[10] https://www.ssllabs.com/ssltest/analyze.html?d=outlook.com&latest abgerufen am 05.07.2019

GMX

GMX hat in Deutschland einen Marktanteil von 24,5%[11] (18 Millionen Nutzer) und ist damit Marktführer unter den E-Mail Providern. Zusammen mit den Schwesteranbieter Web.de (15 Millionen Nutzer) und 1&1 Mail kommen die 1&1 E-Mail Provider auf einen Marktanteil von über 50%. Datenschutz- und Sicherheitsprobleme auf diesem Portal haben deshalb Auswirkungen auf eine große Anzahl Nutzer. Es fällt dabei auf, dass GMX erst im Juni 2019 das 2-Faktor-Authentifizierungs-Feature eingeführt hat[12] und damit Jahre hinter der Konkurrenz wie Hotmail, GMail, Yahoo! zurückliegt. GMX bietet das Versenden von sicheren DE-Mails an[13].

Kritik

GMX steht bei Datenschützern vor allem wegen der offensiven Werbung und der häufigen Vertragsunterbreitung für Website Besucher in der Kritik[14]. Die 2-Faktor-Authentifizierung wurde 2019 erst eingeführt, nachdem zahlreiche Nutzerkonten von Doxern übernommen wurden. Gegen die GMX Serverinfrastruktur gab es in der Vergangenheit mehrfach erfolgreiche Angriffe[15].

Funktionen

GMX bietet als Unternehmen der 1&1 Unternehmensgruppe eine Vielzahl von Diensten, die nicht direkt mit einem E-Mail-Postfach zusammenhängen (z.B. einen eigenen Browser, Handyverträge, Cloud Speicher, eigene Domains, Homepagebaukasten).

Für E-Mail-Postfächer stehen die drei Vertragsoptionen Free, Pro und Top zur Verfügung. In der freien Version stehen 1,5 GB E-Mail Speicherplatz und 20 MB Anhänge pro E-Mail zur Verfügung. Auch 2GB Cloud Speicherplatz werden geboten. Pro und Top erweitern diese Begrenzungen jeweils und fügen einige weitere Features hinzu. Auch das Abschalten von Werbebannern und Popups soll in den bezahlten Versionen enthalten sein.

[11] https://de.statista.com/statistik/daten/studie/151754/umfrage/nutzeranteile-von-e-mail-anbietern-in-deutschland/ abgerufen am 28.06.2019
[12] https://www.heise.de/newsticker/meldung/GMX-fuehrt-sichere-Anmeldung-mit-Zwei-Faktor-Authentifizierung-ein-4439558.html abgerufen am 28.06.2019
[13] https://de-mail.info/ abgerufen am 28.06.2019
[14] https://www.focus.de/digital/internet/nutzer-beschweren-sich-verbraucherschuetzer-warnen-vor-gmx-und-web-de_id_7940035.html abgerufen am 28.06.2019
[15] https://www.heise.de/newsticker/meldung/GMX-Hackerangriff-durch-fatales-Schlupfloch-31708.html abgerufen am 28.06.2019

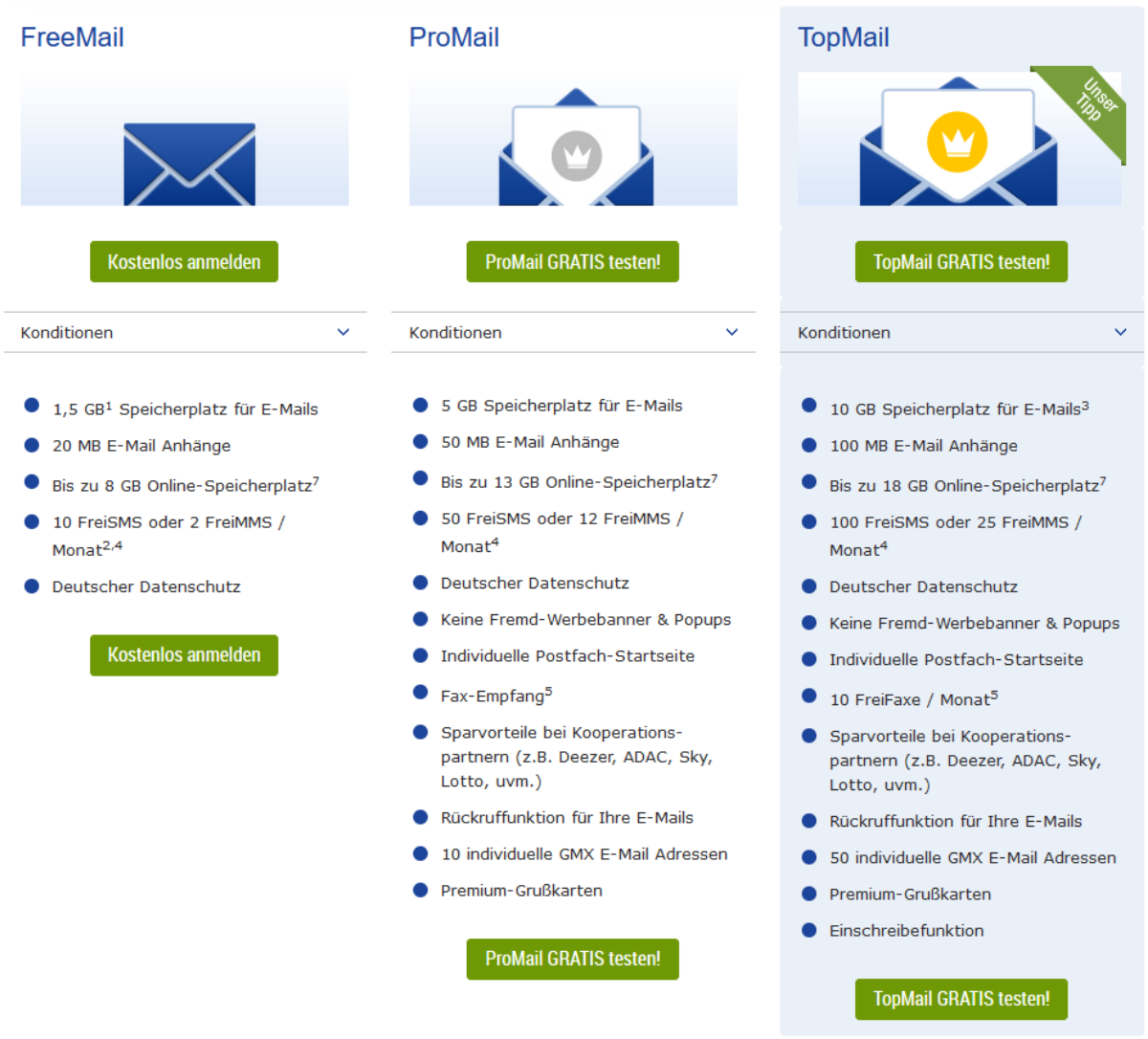


Figure 1: GMX Vergleich der Tarife

Sicherheit

Sowohl auf der Startseite als auch nach einem Login gibt es keinerlei unverschlüsselten Verbindungen zu dem GMX Server, oder zu Drittanbietern. Alle HTTP Aufrufe, aber auch alle nachgeladenen Ressourcen (JavaScript, CSS Dateien, Bilder, Videos, Schriften) werden verschlüsselt übertragen. Eine unverschlüsselte Version der Seite unter http://gmx.de steht nicht zur Verfügung und es erfolgt eine Weiterleitung auf die verschlüsselte Seite. Laut dem SSL Labs Report[16] erhält gmx.de die positive Note A+.

[16] https://www.ssllabs.com/ssltest/analyze.html?d=gmx.de&latest abgerufen am 28.06.2019

GMX bietet seit Juni 2016 Zweifaktorauthentifizierung mittels Authentifizierungsapp an. GMX speichert E-Mails nach eigenen Angaben ausschließlich in deutschen Rechenzentren[17]. Ob die E-Mail Inhalte dort verschlüsselt gespeichert werden ist nicht bekannt. Das Ende-zu-Ende verschlüsselte Senden von E-Mails mit PGP wird unterstützt. Dafür ist Installieren des Drittanbieter Browser Plugins Mailvelope notwendig[18].

Nutzer, die sich 12 Monate lang nicht in ihre Accounts einloggen verlieren ihre E-Mail-Adresse. Dies ist bedenklich, wenn die Adresse neu vergeben wird und weiterhin Nachrichten an den ursprünglichen Nutzer gesendet werden[19].

Erstellen eines Nutzerkontos

Ein GMX Account berechtigt zum Nutzen des Freemail Services, aber auch für das Buchen von Premium Paketen und Domains. Um ein Account anzulegen ist es zwingend erforderlich seine Adresse und sein Geburtsdatum anzugeben. Auch eine zweite E-Mail-Adresse, oder eine Mobilfunknummer muss zur Passwortwiederherstellung angegeben werden. Das Angeben von Sicherheitsfragen zum Zurücksetzen des Passworts, ist nicht mehr erforderlich. Auch Bank- oder Ausweisdaten werden in der freien Version nicht gefordert.

Autor: Jonas Hielscher

> Jonas Hielscher
> benedikt.hielscher@st.ovgu.de

[17] https://www.gmx.net/mail/sicherheit/pgp/#.pc_page.produktseiten.mail.nav_5.sicherheit_pgp abgerufen am 28.06.2019
[18] https://img.ui-portal.de/cms/gmx/produkte/sicherheit/pgp/lp/Anleitung-Verschluesselte-Kommunikation-GMX.pdf abgerufen am 28.06.2019
[19] https://www.nw.de/blogs/games_und_netzwelt/22347107_0rbit-knackte-viele-E-Mail-Konten-Wie-unsicher-sind-GMX-Web.de-und-Co..html abgerufen am 28.06.2019

T-Online

Zahlen und Fakten

T-online Mail, seit einiger Zeit auch Telekom Mail genannt, besitzt im deutschen Markt der E-Mail-Anbieter einen Anteil von 10,8%[20] und wird damit in Deutschland von 1 von 10 E-Mail-Nutzern verwendet. Dadurch können Probleme bei Datenschutz und Sicherheit potenziell einige Millionen Menschen treffen, wodurch die vorhandene Kritik, allen voran die fehlende 2-Faktor-Authentifizierung und Anfälligkeit für Phishing-Attacken, besonders dringlich ist.

Heutzutage muss man den Eindruck von der Startseite t-online.de von dem von den Telekom-Diensten unterscheiden, da t-online.de 2015 von der Telekom an die Ströer Content Group verkauft wurde[21] und damit nun diese, die Webseite verwalten. Stöer betreibt die Startseite heute als Nachrichtenportal, jedoch können Telekom-Kunden dort weiterhin den Zugriff auf ihre E-Mail-Konten und die Telekom-Medien- und Kundencenter vorfinden. Ein Login-Button ist oben rechts auf der Startseite vorzufinden. Der E-Mail-Dienst sowie Medien- und Kundencenter werden weiterhin von der Deutschen Telekom betrieben.

T-online Mail bietet ebenfalls wie GMX sichere DE-Mails an.

Gründung Das Portal wurde im September 1995 gegründet.

Kritik Obwohl sich Ratgeber im Allgemeinen dazu auf den Telekom-Hilfeseiten finden lassen[22], bietet die Telekom selber bis heute noch keine 2-Faktor-Authentifizierung[23] für ihre Dienste an. Darüber beschweren sich die Nutzer in Foren und es herrschen Diskussionen[24]. Zwar wurde am 22.01.2019 offiziell im Forum verlauten lassen, dass diese Funktion wohl demnächst “generell für alle Telekom Login Seiten eingeführt” werden soll[25], bis heute hat sich aber noch nichts getan. Damit liegt T-online Mail in diesem Bereich weit hinter der Konkurrenz, wie GMX, Hotmail, GMail und Yahoo!, zurück, die dies seit einem bzw. mehreren Jahren anbieten. Dies ist besonders bedauerlich, da T-online Kunden schon Ziele von Phishing-Attacken wurden[26], wobei 2-Faktor-Authentifizierung eine wichtige zusätzliche

[20] https://de.statista.com/statistik/daten/studie/151754/umfrage/nutzeranteile-von-e-mail-anbietern-in-deutschland/ abgerufen am 28.06.2019
[21] http://www.manager-magazin.de/unternehmen/it/stroeer-kauft-t-online-a-1047997.html abgerufen am 22.05.2019
[22] https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicher-digital/details/zwei-faktor-authentifizierung-540852 abgerufen am 01.07.2019
[23] https://www.golem.de/news/stiftung-warentest-zweiter-faktor-bei-immer-mehr-internetdiensten-verfuegbar-1903-140012.html abgerufen am 01.07.2019
[24] https://telekomhilft.telekom.de/t5/E-Mail-Center/Warum-gibt-es-noch-keine-2-Faktor-Authentifizierung-bei-der/td-p/3680345/page/1 abgerufen am 01.07.2019
[25] https://telekomhilft.telekom.de/t5/E-Mail-Center/Telekom-Mail-2-Faktor-Authentifizierung/td-p/3612865 abgerufen am 01.07.2019
[26] https://www.t-online.de/digital/sicherheit/id_85126212/phishing-vorsicht-vor-falschen-mails-in-namen-von-t-online-de-.html abgerufen am 01.07.2019

Schutzmaßnahme darstellen würde. Leider fehlt ebenso eine Funktion, sich E-Mails bei einem Login von einem neuen, unbekannten Gerät zuschicken zu lassen, um eventuelle Übernahmeversuche erkennen zu können.[27] Datenschützer kritisieren die aufdringliche und massenhaft eingebundene Werbung und Trackingmaßnahmen, die ebenso von Ströer auf der Startseite wie auch von der Telekom im Postfach vorzufinden sind. Dazu kommt die automatische Anmeldung zum Telekom Freemail Newsletter bei Registrierung, wodurch Vertragsunterbreitungen direkt im Postfach landen.

Funktionen

Die Telekom bietet viele verschiedene Dienste an, darunter Kundencenter als Verwaltungshub, Mail, Magenta-Dienste, wie MagentaCloud und MagentaMusik, sowie Mobilfunk-, Festnetz-, Internet- und TV-Tarife. Für die einfache Verwaltung aller in Anspruch genommenen Dienste und den bequemen Wechsel zwischen ihnen auf dem Gerät, gibt es den Telekom Login. So soll man sich nur einen Benutzernamen und ein Passwort merken müssen, zum Zwecke des Komforts. Als Nutzer von T-online Mail kann man zwischen 2 Vertragsoptionen wählen. Freemail ist kostenlos und bietet 1 GB Postfachspeicher sowie die Möglichkeit bis zu 100 Mails pro Tag bzw. 1.000 Mails pro Monat versenden zu können. Dazu soll ein Spamschutz der Telekom das Postfach rein halten. Mail M ist die Premiumoption "für höchste Ansprüche" für 2,95 € monatlich. Dadurch bekommt man Zugriff auf 15GB Speicher, den konfigurierbaren "Spamschutz Plus" und die Möglichkeit 5000 Mails pro Tag zu verschicken. Außerdem soll so die Werbung im Postfach ausgeschalten werden[28].

Sicherheit

Eigene Angaben Die Telekom ist Gründungsmitglied der Brancheninitiative "E-Mail made in Germany". Dadurch sind bei T-online Mail Sicherheitsmaßnahmen, auf die sich die großen E-Mail-Anbieter geeinigt haben, kostenlos automatisch aktiviert und nicht abschaltbar. So sollen alle Mails immer SSL-verschlüsselt übermittelt werden und nur in gesicherten Rechenzentren in Deutschland und nach strengen deutschen Datenschutzstandards gespeichert sein[29]. Dies wird zwischen den Mitgliedern der Initiative, also Telekom, GMX, Web.de, Freenet, 1&1 und Strato, garantiert.[30]. Leider bleibt offen, ob die Mails in den Rechenzentren auch verschlüsselt gespeichert werden. Es wird darauf hingewiesen, darauf zu achten, dass SSL-Verschlüsselung vom jeweiligen Endgerät und Programm unterstützt wird[31].

Darüber hinaus unterstützt T-online Mail sogar DE-Mail, welches eine weiter entwickelte Version der "E-Mail made in Germany" sein soll. Diese soll neben der sicheren Datenübertragung und der Verar-

[27] https://telekomhilft.telekom.de/t5/E-Mail-Center/Warum-gibt-es-noch-keine-2-Faktor-Authentifizierung-bei-der/td-p/3680345/page/1 abgerufen am 01.07.2019
[28] https://www.telekom.de/unterwegs/apps-und-dienste/kommunikation/telekom-e-mail abgerufen am 28.06.2019
[29] https://kommunikationsdienste.t-online.de/email-made-in-germany/ abgerufen am 30.06.2019
[30] https://kommunikationsdienste.t-online.de/email-made-in-germany/ abgerufen am 30.06.2019
[31] http://kommunikationsdienste.t-online.de/email/verschluesselung/ abgerufen am 01.07.2019

beitung der Daten in deutschen Rechenzentren zusätzlich die einwandfreie Identität von Sender und Empfänger gewährleistet.[32] DE-Mail Sendungen sollen dadurch gesetzlich rechtssicher sicher. [^deMail-Telekom]. Dafür ist eine kostenlose Anmeldung für DE-Mail mithilfe der eigenen t-online.de-Adresse unter https://www.de-mail.t-online.de nötig.

Unverschlüsselte Verbindungen Alle Inhalte im Login-Bereich und im Postfach, sowohl von T-online-Servern als auch von Drittanbietern, werden über verschlüsselte Verbindungen übertragen. Chromium Übersicht der Verschlüsselung bei Übertragungen

Nachfolgend wurden einige Eigenschaften der Webseite “email.t-online.de” zusätzlich mit entsprechenden Online-Tools untersucht. Dabei ist zu beachten, dass ein Browser ohne eingeloggten Nutzer bei Aufruf von email.t-online.de auf die Startseite t-online.de weitergeleitet wird, um sich über den Login-Button anmelden zu können. Dies kann die Tests der Online-Tools verfälschen, da sie eine Website testen, die theoretisch von einem anderen Anbieter verwaltet wird.

Bei einem Verbindungsversuch über das unverschlüsselte http://email.t-online.de wird automatisch auf die verschlüsselte Version weitergeleitet, vorausgesetzt man ist eingeloggt. Ansonsten landet man auf immerhin auf der verschlüsselten Version der Startseite.[^httpstatus]

Dem Qualys SSL Labs Report zufolge[^sslLabTonline], bietet email.t-online.de mit einem A+ Score eine sehr gute Unterstützung aktueller Sicherheitsfunktionen in der Datenübertragung im Browser.

Laut hstspreload verwendet zumindest t-online.de kein HSTS[^hsts]. Email.t-online.de kann nicht über dieses Tool geprüft werden, da Subdomains nicht unterstützt werden. Es ist unklar, ob die Erkenntnis übertragbar ist, da die Subdomain von einem anderen Anbieter verwaltet wird.

Schutz vor Spam und auch Viren soll der eingebaute Spam-Schutz absichern[33]. Dadurch sollen unerwünschte und gefährliche E-Mails erst gar nicht in den Posteingang gelangen.

Eine Ende-zu-Ende-Verschlüsselung von versendeten Mails über PGP ist möglich, allerdings muss dazu das Browser-Plugin Mailvelope von einem Drittanbieter installiert werden[34].

Die Passworterstellung erfordert die Erfüllung von gewissen Sicherheitskriterien und lässt dadurch beliebte schwache Passwörter nicht zu. Das Passwort muss mindestens 8 Zeichen und mindestens 2 der folgenden Bedingungen erfüllen: Kleinbuchstaben, Großbuchstaben, Ziffern, Sonderzeichen. Damit ist allerdings immer noch zum Beispiel “Passwort” möglich. Außerdem darf ein Passwort maximal 16 Zeichen lang sein, was eine veraltete unnötige Begrenzung darstellt.

[32] https://de-mail.info/ abgerufen am 28.06.2019
[33] https://www.telekom.de/unterwegs/apps-und-dienste/kommunikation/telekom-e-mail abgerufen am 28.06.2019
[34] https://www.t-online.de/digital/sicherheit/id_73814894/mailvelope-sichere-e-mail-verschluesselung-geht-auch-einfach.html abgerufen am 01.07.2019

Erstellen eines Nutzerkontos

Für die Nutzung des T-online Mailingdienstes wird ein Telekom Account benötigt. Somit ist man dann im Besitz eines All-in-One-Accounts für das Telekom-Ökosystem, selbst wenn man nur Interesse am Mailingdienst hat. Als Telekom-Vertragskunde liegt solch ein Account oft schon vor. Für die Erstellung wird die Angabe eines Geburtsdatums benötigt. Leider werden aufgrund der “Passwort vergessen”-Funktion eine Antwort auf eine Sicherheitsfrage sowie eine, im Schritt danach per SMS zu verifizierende, Mobilfunknummer gefordert. Bank- oder Ausweisdaten werden in der freien Version allerdings nicht gefordert.

> Niklas Baier
> niklas.baier@st.ovgu.de

[^deMailTelekom] https://www.telekom.de/zuhause/de-mail abgerufen am 01.07.2019:[35] https://de-mail.info/ abgerufen am 28.06.2019 [^sslLabTonline]: https://www.ssllabs.com/ssltest/analyze.html?d=email.t-online.de zuletzt abgerufen am 02.07.2019 [^hsts]: https://hstspreload.org/?domain=t-online.de zuletzt abgerufen am 02.07.2019 [^httpstatus]: https://httpstatus.io/ zuletzt abgerufen am 02.07.2019

[35] https://de-mail.info/ abgerufen am 28.06.2019

Vorgehensweise

Um diese E-Mail-Anbieter daraufhin zu analysieren, ob die Nutzung bedenklich für den Datenschutz sein kann, werden wir die hier erläuterte Vorgehensweise auf Grundlage bestimmter Szenarien (was wir tun) und Kriterien (was wir beobachten) einsetzen, um alle analysierten Anbieter sachlich vergleichen zu können.

Versuchsaufbau

Ein Versuch ist für uns das Durchspielen eines Szenarios in einer leeren, ungehärteten Chrome-Sitzung, zusammen mit der Analyse der Unterschiede unter verschiedenen weiteren Umständen (siehe "Ablauf eines Versuchs").

Browser

Chromium Wir führen den Versuch in erster Linie mit Chromium in der aktuellsten Version durch, da dieser Browser die Ansicht von Nachrichten in Websocket-Verbindungen ermöglicht. Zusätzlich benötigen wir die Erweiterung "uMatrix"[36], um die Zahl und Domains der Drittanbieter einfach sehen zu können.

Oben rechts gibt es ein Benutzermenü mit dem Eintrag "Nutzer verwalten", über den die Profile verwaltet werden können. Hier können wir vor jeder Versuchsreihe ein neues, unbenutztes Profil anlegen, damit die Versuche wiederholbar sind.

Firefox Wir verwenden zusätzlich Firefox, um Unterschiede zwischen Browsern zu testen. Zudem möchten wir überprüfen, wie effektiv die Firefox-Funktion zur Blockierung der Aktivitätenverfolgung das Tracking durch die E-Mail-Provider verhindert. Zusätzlich benötigen wir auch hier "uMatrix."[37]

Der Befehl `firefox --ProfileManager --new-instance` startet den Profilmanager (kann ausgeführt werden mit `Windowstaste+R`, oder `Alt+F2` in Linux), in dem wie in Chromium unbenutzte Profile angelegt werden können.

Gehärteter Browser Um eine Empfehlung für möglichst viele Endnutzer aussprechen zu können, verwenden wir Firefox mit der Einstellung "Streng" unter "Datenschutz & Sicherheit" als einzige Härtung unseres Browsers. Wir wollen so testen, ob es eine einfache Möglichkeit gibt, Tracking bei einem Anbieter zu entgehen.

[36] https://chrome.google.com/webstore/detail/umatrix/ogfcmafjalglgifnmanfmnieipoejdcf?hl=de; aufgerufen am 04.07.2019
[37] https://addons.mozilla.org/de/firefox/addon/umatrix/; aufgerufen am 04.07.2019

Zu vergleichende Szenarien

Betrachtet werden die *Anmeldung* bei einem Anbieter (ab dem Besuch der Anmeldeseite bis zum Absenden der Login-Daten), der *Versand* einer E-Mail (ab dem Klick auf den Senden-Button) sowie der *Empfang & Abruf* einer beliebigen E-Mail (Posteingang & E-Mail-Ansicht).

Ablauf eines Versuchs

uMatrix ist stets auf "Alles erlauben" einzustellen. Zu jedem Szenario gibt es für jedem Anbieter drei Versuche: jeweils einen in Google Chrome, in Firefox, und im gehärteten Browser. Die letzten zwei werden für die Analyse der "Unterschiede in Firefox" und der "Effektivität der Browserhärtung" benötigt.

Für jeden Versuch müssen wir zuerst mit F12 die Developer-Tools öffnen, und im Tab "Netzwerk" (oder "Netzwerkanalyse") das automatische Leeren der Logs deaktivieren. Nun wird das Szenario durchgespielt und daraufhin die entstandenen Daten nach den folgenden Kriterien ausgewertet.

Jeder Versuch wird zur Nachvollziehbarkeit mit Screenshots des uMatrix-Fensters dokumentiert (siehe dazu "Anhang 1"), zusammen mit der jeweilige exakten Vorgehensweise und den Ergebnissen.

Zu vergleichende Kriterien

Drittanbieter *Wie viele und welche Drittanbieter können an private Daten des Nutzers gelangen?*

Die von uMatrix angezeigte Liste wird hierfür verwendet, zusätzlich werden falls vorhanden Drittanbieter in die Liste aufgenommen, die nur in der Datenschutzerklärung vorkommen.

Ergebnis: Anzahl der Drittanbieter; Liste mit Domains der Unternehmen

Versandte Daten *Wie viele und welche Daten werden tatsächlich an einen Drittanbieter versendet?*

Die Netzwerkverkehrsansicht in den Developer-Tools wird nach der Drittanbieter-Domain gefiltert, um die Datenmenge auswerten zu können. Der Zweck der Daten wird falls möglich den Angaben auf der offiziellen Drittanbieter-Webseite entnommen.

Ergebnis (je Drittanbieter): Größe in KiB; Zweck der Daten

Sessions *Setzen Drittanbieter z. B. Cookies ein, um ihrerseits Nutzer eindeutig zu identifizieren?*

Wir können dies im "Anwendung"-Tab in Chromium und im "Speicher"-Tab in Firefox sehen. Gibt es hier einen scheinbar zufällig generierten Token, identifiziert der Drittanbieter den Nutzer auf eine eindeutige Art und Weise.

Ergebnis (je Drittanbieter): ja/nein (nein bevorzugt)

Schweregrad *Wie kritisch sind die übertragenen Daten im schlechtesten Fall?*

Dies kann aus versandten Daten abgeleitet werden; aufgrund des Umfangs gehen wir nur auf auffällige Verbindungen ein. Eine Herabstufung erfolgt bei Drittanbieter-JavaScript-Inhalten, die im Hauptkontext ausgeführt werden, da diese vollen Zugriff auf alle Inhalte haben - bei aktiviertem “Group by Frame” in Chromium erscheinen diese Skripte in der obersten Ebene. Gibt es nur Anbieter, die direkt im Quellcode der Seite zu finden sind, wird eine Note abgezogen, ansonsten erfolgt eine Herabstufung auf Note 5.

Ergebnis (Schulnote 1-5): **[1]** keine Drittanbieter oder nur IP-Adressen & Browserinformationen (bevorzugt); **[2]** persönliche Session; **[3]** persönlich identifizierbare Informationen (beispielsweise Name oder E-Mail-Adresse); **[4]** Absender oder Betreffzeilen von E-Mails; **[5]** Inhalte von E-Mails

Unterschiede in Firefox Gibt es Unterschiede bei der Verwendung in Firefox?

Dies weisen wir mit der von uBlock angezeigten Anzahl der Drittanbieter nach.

Ergebnis: Differenz “Drittanbieter Firefox” - “Drittanbieter Chrome” (nahe an 0 bevorzugt)

Effektivität der Browserhärtung Werden tatsächlich keine Daten mehr an Drittanbieter versendet, wenn man einen gehärteten Browser surft? Wenn nein, welche Drittanbieter sind davon betroffen?

Dies testen wir mithilfe der von uBlock angezeigten Liste geladener Drittanbieter..

Ergebnis: Anzahl & Liste übriger Drittanbieter (keine bevorzugt)

Vollständigkeit Werden nur in der Datenschutzerklärung explizit erwähnte Anbieter kontaktiert?

Wird einem Anbieter das Recht eingeräumt, selbst zu entscheiden, welche weiteren Anbieter Zugang zu Daten erhalten können, wird dieser Punkt mit “nein” beantwortet.

Ergebnis: ja/nein (ja bevorzugt)

Transparenz Wie verständlich sind die Datenschutzbestimmungen formuliert?

Dieses an sich subjektive Kriterium soll durch eine Einteilung in genauer spezifizierte Schulnoten möglichst objektiv gehalten werden:

Ergebnis (Schulnote 1-5): **[1]** vereinfachte Version verfügbar; **[2]** kurz und einfache Sprache; **[3]** mit genug Zeit nachvollziehbar; **[4]** unnötig lang oder kompliziert; **[5]** für Laien unverständlich

> Moritz Marquardt
> moritz.marquardt@st.ovgu.de

Durchführung und Ergebnisse

Google Mail

Versuchsprotokoll

Die Untersuchung von Google Mail wurde unter Windows 10 (Version 1809 - Enterprise) im IP Adressbereich der Otto-von-Guericke-Universität Magdeburg durchgeführt. Für die Mehrzahl der Untersuchungen wurde ein neu installierter Chromium Browser verwendet (Version 77.0.3824.0).

Ergebnisse

Google Mail zeigt keinerlei Werbungen ohne Zulassung des Nutzers.

Drittanbieter App-Entwickler, die Teil des Gmail-Programms von Google sind, dürfen diese E-Mails unter bestimmten Umständen lesen, um neue Dienste oder App-Funktionen zu erstellen, heißt es. Der Großteil der E-Mails würde automatisch per Computersoftware gescannt, in einigen Fällen sollen aber menschliche Mitarbeiter mitgelesen haben. Return Path, ein Unternehmen, das sich E-Mail-Marketing auf die Fahnen geschrieben hat, hat angeblich die Posteingänge von mehr als 2 Millionen Menschen gescannt und 8000 E-Mails ausspionieren lassen.

Versandte Daten Durch das Anfertigen und Absenden von E-Mails werden keine Daten aus dem Browser gesendet. Der Inhalt von der geschriebenen E-Mail wird lediglich per Post Request an einen G-Mail Server versendet.

Verschlüsselung Mit S/MIME wird eine E-Mail verschlüßelt und während der Zustellung unterstützt. Die ausgehenden E-Mails werden automatisch verschlüsselt, wann immer dies möglich ist.

Datenschutz, Transparenz

- Die personenbezogenen Daten einschließlich der Gmail- und Google-Kontoinformationen werden von Google nicht verkauft. Sie geben keinerlei personenbezogene Daten an Werbetreibende weiter, es sei denn, der Nutzer wünscht dies.
- Sie achten außerdem sehr sorgfältig auf die Art der Inhalte, für die sie Werbung schalten. Google wird beispielsweise keine Werbung auf der Grundlage sensibler Informationen wie Hautfarbe, Religion, sexueller Orientierung, Gesundheit oder sensibler Finanzdaten schalten. Die in Gmail geschaltete Werbung unterliegt den Gmail-Werberichtlinien.

- Wenn der Nutzer festlegen möchte, dass keine auf Ihren personenbezogenen Daten basierende Werbung für ihn in Gmail angezeigt wird, rufen er die Seite “Einstellungen für Werbung” auf und deaktivieren Sie dann die Option “Weitere Werbung deaktivieren”. Wenn der Nutzer diese Funktion deaktiviert, kann es dennoch vorkommen, dass Gmail-Werbung eingeblendet wird. Diese bezieht sich jedoch nicht mehr auf personenbezogene Daten, die mit Ihrem Google-Konto verknüpft sind. https://codeberg.org/ovgu/itsec-email-comparison/src/branch/master/paper/images/GmailDatenschutz.png

Rawan Jouli
rawan.jouli@st.ovgu.de

Outlook

Ergebnisse

Drittanbieter & versandte Daten Outlook.com verwendet Inhalte von 14 Drittanbieter-Domains, davon sind allerdings 7 von Microsoft selbst und werden für die weitere Auswertung ignoriert.

- live.com (Microsoft)
- adnxs.com
- advertising.com
- bing.com (Microsoft)
- fonts.googleapis.com
- gstatic.com
- microsoft.com (Microsoft)
- office365.com (Microsoft)
- olsvc.com (Microsoft)
- scorecardresearch.com
- skype.com (Microsoft)
- skypeassets.com (Microsoft)
- taboola.com
- yahoo.com

Versandte Daten

- adnxs.com: AppNexus, Tracking für Werbezwecke (29 KB)
- advertising.com: Verizon, Vermittlung von Werbung (417 B)
- fonts.googleapis.com: Google Fonts, Schriftarten (215 KB)
- gstatic.com: Google CDN (215 KB)
- scorecardresearch.com: Tracking & Umfragen (12 KB)
- taboola.com: Vermittlung von Werbung (51 KB)
- yahoo.com: Vermittlung von Werbung (904 B)

Sessions Ja, Taboola speichert eine eindeutige User ID namens “taboola global:user-id” unter adnxs.com

Schweregrad Da geöffnete E-Mails eine eindeutige ID haben, die in der URL steht, und Drittanbieter Zugriff auf die URL in Form des Referers haben, erhält Outlook.com eine 4. Da Skripte von adnxs.com als Drittanbieter direkt im Seitenkontext geladen wird, wird Outlook.com auf eine 5 heruntergestuft.

Unterschiede in Firefox In Firefox gibt es gleich viele Drittanbieter, wobei in beiden Browsern die Anzahl von Aufruf zu Aufruf schwankt.

Effektivität der Browserhärtung Es werden bei aktivierter Browserhärtung immer noch adnxs.com, advertising.com und yahoo.com (also 3 Drittanbieter) verwendet, die jedoch ihrerseits keine weiteren Inhalte nachladen.

Vollständigkeit Dieser Punkt muss mit nein beantwortet werden, da weiteren Werbefirmen wie beispielsweise Yahoo das Recht eingeräumt wird, Daten ihrerseits beliebig weiterzuverwenden.

Transparenz Die Datenschutzbedingungen sind stark verschachtelt und relativ lang - um die kompletten Bedingungen zu lesen, muss man sehr viele Blöcke manuell ausklappen. Hat man das mal geschafft, ist die komplette Seite jedoch relativ leicht verständlich. Damit gibt es die Note 4.

Moritz Marquardt
moritz.marquardt@st.ovgu.de

GMX

Versuchsaufbau

Die Untersuchung des GMX Web Mail Clients wurde unter Windows 10 (Version 1809 - Enterprise) im IP Adressbereich der Otto-von-Guericke-Universität Magdeburg durchgeführt. Für die Mehrzahl der Untersuchungen wurde ein neu installierter Chromium Browser verwendet (Version 77.0.3824.0). An den Voreinstellungen des Browsers wurden keine Veränderungen vorgenommen. Als einziges zusätzlich installiertes Plugin kam uMatrix für Chrome[38] (Version 1.3.16) zum Einsatz. Dieses Plugin wurde so eingestellt, dass es Verbindungen visualisiert, jedoch nicht blockiert.

Einige Testergebnisse wurden mit zwei anderen Set-ups verglichen.

1. Chromium Browser mit voll aktiviertem uMatrix Plugin.
2. Neu installiertem Firefox Developer Browser (Version 68.0b10 64bit), an dem keinerlei Änderungen vorgenommen und keine Plugins installiert wurden.

Ergebnisse

Das GMX Portal zeigt offensichtlich auf jeder Seite große Mengen an Drittanbieter Werbung an. Ein Aufruf der Startseite von gmx.net lädt im Schnitt 5,5 MB unterschiedlicher Medien herunter. Eine Untersuchung durch PrivacyScore zeigt 21 bekannte Tracker auf der Startseite, jedoch keine bekannten Sicherheitslücken[39].

Drittanbieter

Nach einem Login und während des Lesens und Schreibens von E-Mails sind sehr viele Drittanbieter Ressourcen in die Websites eingebunden. Direkt nach einem Login ist die Anzahl noch geringer. Eine genaue Übersicht über alle Drittanbieter und eine Reproduktion der Ergebnisse ist schwer, da sich diese nach jedem Neu laden der Seite ändern (es werden andere Werbepartner eingebunden). Im Folgenden eine Übersicht über alle geladenen Ressourcen in E-Mail-Verfassen-View, aufgezeichnet am 12. Juni 2019. Die Ressourcen umfassen die Kategorien: CSS, Grafik, Medien, Skripte, XHR-Calls, Frame und Sonstige, wobei die XHR Calls als **REST Calls** besonders ausgewiesen sind, da sie besonders viele Daten transportieren können:

- 1rx.io: 2
- 2mdn.net: 9

[38] https://chrome.google.com/webstore/detail/umatrix/ogfcmafjalglgifnmanfmnieipoejdcf?hl=de abgerufen am 28.06.2019
[39] https://privacyscore.org/site/30819/ abgerufen am 28.06.2019

- ad-sev.net: 5
- adform.net: 32
- adition.com: 28
- adnxs.com: 62 (davon 1 REST Call)
- adsrvr.org: 6
- adsrvx.com: 20
- amazon-adsystem.com: 19 (davon 9 REST Calls)
- atdmt.com: 2
- bing.com: 4
- bitdefender.de: 2
- casalemedia.com: 16
- cloudflare.com: 1
- conrad.de: 3
- criteo.com: 10 (davon 8 REST Calls)
- criteo.net: 2 (davon 1 REST Call)
- research.de.com: 20
- de17a.com: 4
- doublecklick.net: 54 (davon 4 REST Calls)
- exactag.com: 3
- facebook.com: 1
- gmxpro.net: 25 (davon 1 REST Call)
- google-analytics.com: 1
- google.com: 4
- google.de: 1
- googlesyndication.com: 32
- gstatic.com: 6
- ioam.de: 8
- lijit.com: 3
- m6r.eu: 4
- mathtag.com: 5
- media1.eu: 3
- mookie1.com 19
- mxcdn.net: 1
- myvisualiq.net: 5
- openx.net: 21 (davon 8 REST Calls)
- pubmatic.com: 6 (davon 1 REST Call)
- rifihub.com: 5
- rubiconproject.com: 1

- serving-sys.com: 36 (davon 4 REST Calls)
- simpli.fi: 3
- sitecount.com: 1
- smartadserver.com: 12 (davon 1 REST Call)
- spotchange.com: 3
- tapad.com: 5
- tidaltv.com: 4
- tifbs.net: 2
- turn.com: 3
- ui-portal.de: 30 (davon 2 REST Calls)
- uimserv.net: 22
- w55c.net: 7
- wayfair.com: 3
- yahoo.com: 4
- yieldlab.net: 5
- youtube.com: 1
- zanox.affiliate.de: 3
- zanox.com: 6

Es wurden bei diesem Test in Summe also 595 Ressourcen von Drittanbietern geladen. Davon waren 40 Ressourcen API Calls gegen Drittanbieter Schnittstellen, die potentiell eine größere Menge an Daten übertragen haben. Inklusive der Inhalte die direkt von gmx.net kamen wurden 7,3 MB heruntergeladen und 1,1 MB hochgeladen und zwar ab dem Zeitpunkt ab dem auf **E-Mail Verfassen** geklickt wurde, über 2 Wechsel aus dem Tab hinaus, bis sich die Seite vollständig geladen hat. Interessant dabei ist, dass nach jedem Wechsel aus dem Browser Tab (entweder in einen anderen Tab, oder aus dem Browser heraus) zahlreiche Drittanbieter Ressourcen nachgeladen werden.

Unter den Drittanbietern sind bekannte Tracker, wie doublecklick.net und die meisten der großen US-Amerikanischen Webunternehmen: Google, Facebook, Microsoft (mit Bing), yahoo!, youtube. Werbetreibende laden ihre Ressourcen teilweise direkt in die Seite (z.B. conrad.de).

Nach jedem Zurückwechseln in den GMX Tab werden zahlreiche Ressourcen nachgeladen

Versandte Daten

Während der Untersuchung des GMX Webportals konnte zu keinem Zeitpunkt festgestellt werden, dass Echtzeitdaten aufgezeichnet, oder versendet werden. Es werden zwar viele bekannte Tracker eingebunden. Jedoch konnte nicht nachgewiesen werden, dass diese das Nutzerverhalten mitschneiden. Sehr wohl aber werden Werbebanner mit eindeutigen IDs geladen.

GMX erhält hierfür die Schulnote 2, da keine Nutzerdaten jenseits von Session Daten direkt an Drittanbieter versendet werden.

Mail Versand

Während des Verfassens und Absendens von E-Mails werden keinerlei Daten aus dem Browser gesendet (weder über Websocket-Verbindungen noch über API Calls). Der Inhalt der geschriebenen E-Mail wird lediglich per Post Request an einen GMX Server versendet.

Sessions

Es werden zu keinem Zeitpunkt Cookies von Drittanbietern gesetzt. Auch der LocalStorage wird nicht durch Drittanbietern befüllt. GMX selber jedoch setzt zahlreiche Cookies, die zur eindeutigen Identifizierung eines Nutzers geeignet sind.

Auf gmx.net werden keine Drittanbieter Cookies und Lokale Daten gespeichert

Öffnen von E-Mails

Beim Öffnen von E-Mails werde sofort alle Ressourcen (Bilder, Scripte, Fonts, etc.) aus der E-Mail geladen. Ein Tracking ist somit einfach möglich.

Verschlüsselung

Der Aufruf der Domain gmx.de leitet automatisch auf gmx.net weiter. gmx.net steht ausschließlich als verschlüsselte Version zur Verfügung. Keine Ressourcen werden unverschlüsselt übertragen. Dies umfasst alle API Calls, Medien, JavaScript, CSS Dateien und Fonts von GMX und Drittanbietern.

Effektivität der Browserhärtung

Das Aktivieren des Browser Plugins uMatrix blockiert das Nachladen aller Drittanbieter Inhalte. GMX weist in diesem Fall mit einem Banner daraufhin, dass JavaScript zur Verwendung der Website eingeschaltet werden soll. Dies ist eine Falschmeldung, da JavaScript lediglich für Drittanbieter blockiert, generell im Browser jedoch zugelassen ist. Die Benutzung der E-Mail Dienste funktioniert auch ohne das Nachladen von Drittanbieterinhalten. Beim Aufruf der Startseite fällt dabei auf, dass GMX lediglich von `ui-portal.de` nachladen möchte, wenn das Plugin aktiviert ist. Andere Verbindungsversuche werden nicht unternommen. Zahlreiche Werbebanner zeigen keine Bilder. Die übertragene Datenmenge reduziert sich von ca. 5,5 MB auf ca. 1,2 MB.

Unterschiede in Firefox

Es konnte in keinem der Szenarien ein signifikanter Unterschied zwischen einem nicht modifizierten Firefox und einem Chromium Browser festgestellt werden. Ein exakter Vergleich ist aufgrund des fehlenden Determinismus der Drittanbietereinbindungen nicht möglich. Die bekanntesten Tracker (z.B. doublecklick.net) wurden in beiden Browsern nicht geblockt.

Datenschutzrichtlinien

GMX wirbt offensiv mit deutschen Datenschutzstandards. Beim Aufruf der Startseite wird auf die Verwendung von Cookies hingewiesen, jedoch gibt es keine weiteren Einstellungen für die Cookies.

Transparenz der Richtlinien

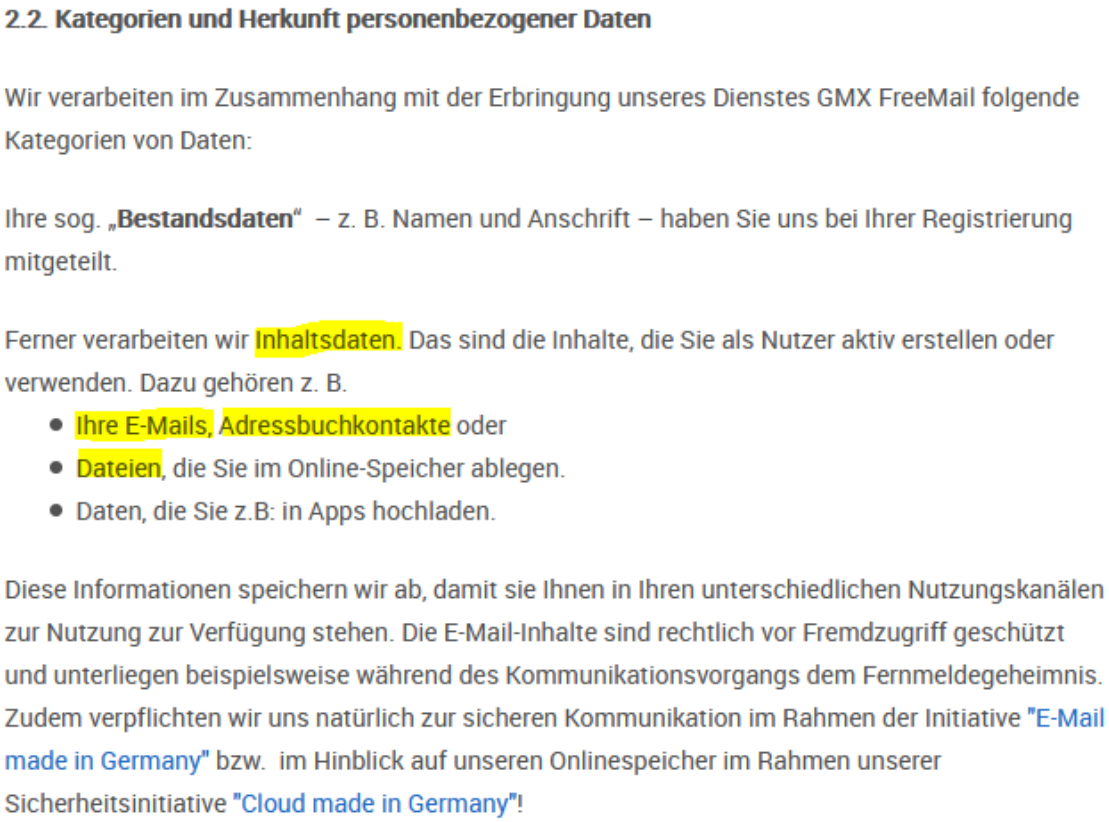
Die GMX Datenschutzerklärung besteht aus ca. 13,900 Wörtern und fasst die Bestimmungen für mehrere Angebote (z.B. Media Center und Freemail) zusammen[40]. In Abschnitt 2.2. erklärt GMX, dass Inhaltsdaten, also E-Mails, Kontakte und hochgeladene Daten verarbeitet werden. Es ist nicht ersichtlich ob dies bedeutet, dass die Daten einfach nur gespeichert werden, oder ob sie zur weiteren Analyse des Nutzerverhalten herangezogen werden. Allerdings wird in Abschnitt 2.4. erklärt, dass generell Analysewerkzeuge zum Einsatz kommen.

GMX zeigt personalisierte Werbung an. Es ist möglich dies abzuschalten. Der Weg zu dieser Abschaltung ist versteckt hinter: `GMX Mein Account` > `Kommunikationsprofil` > `Nutzungsbasierte Werbung`. In wie weit die Abschaltung funktioniert wurde im Rahmen dieser Arbeit nicht analysiert.

Beim Benutzen des Online Portals speichert GMX den Verlauf der Session. Dies umfasst u.a. das Speichern von Aufrufen einzelner Elemente auf der Seite (vergleiche Datenschutzrichtlinien Abschnitt 3.1.2). Eine Abschaltung oder Teilabschaltung von Cookies ist nicht möglich.

GMX erhält hierfür die Schulnote 3, da die Bestimmungen zwar ohne Fremdwörter auskommen, aber dennoch wichtige Sektionen nicht hervorheben.

[40] https://agb-server.gmx.net/datenschutz#datenschutz_freemail abgerufen am 28.06.2019



2.2. Kategorien und Herkunft personenbezogener Daten

Wir verarbeiten im Zusammenhang mit der Erbringung unseres Dienstes GMX FreeMail folgende Kategorien von Daten:

Ihre sog. „**Bestandsdaten**“ – z. B. Namen und Anschrift – haben Sie uns bei Ihrer Registrierung mitgeteilt.

Ferner verarbeiten wir Inhaltsdaten. Das sind die Inhalte, die Sie als Nutzer aktiv erstellen oder verwenden. Dazu gehören z. B.

- Ihre E-Mails, Adressbuchkontakte oder
- Dateien, die Sie im Online-Speicher ablegen.
- Daten, die Sie z.B: in Apps hochladen.

Diese Informationen speichern wir ab, damit sie Ihnen in Ihren unterschiedlichen Nutzungskanälen zur Nutzung zur Verfügung stehen. Die E-Mail-Inhalte sind rechtlich vor Fremdzugriff geschützt und unterliegen beispielsweise während des Kommunikationsvorgangs dem Fernmeldegeheimnis. Zudem verpflichten wir uns natürlich zur sicheren Kommunikation im Rahmen der Initiative "E-Mail made in Germany" bzw. im Hinblick auf unseren Onlinespeicher im Rahmen unserer Sicherheitsinitiative "Cloud made in Germany"!

Figure 2: GMX verarbeitet laut den Datenschutzbestimmungen den Inhalt von E-Mails, Kontakten und Dateien

Fazit

GMX trackt Nutzer um personalisierte Werbung anzeigen zu können. Dies ist in den Datenschutzbestimmungen eindeutig definiert und kann der DSGVO entsprechend abgeschaltet werden. Die große Anzahl an Werbung durch Drittanbieter auf allen Seiten erweckt sehr schnell einen unseriösen Eindruck und kann Einfalltor für Schadcode sein. Dennoch erfüllt die Website auf Client Seite gängige Sicherheitsanforderungen, da alle Daten verschlüsselt übertragen werden. Auch wird auf der Seite selbst das Verhalten nicht live getrackt, z.B. in Form von Tastenanschlägen. Sehr wohl jedoch gibt es personalisierte Angebote und Drittanbieter erfahren potenziell, wenn Nutzer E-Mails lesen, oder versenden. Über den Inhalt der empfangenen, oder verfassten E-Mails haben sie jedoch keinerlei Kenntnis.

Jonas Hielscher
benedikt.hielscher@st.ovgu.de

T-Online

Versuchsprotokoll

Ergebnisse

Drittanbieter

Versandte Daten

Sessions

Schweregrad

Verschlüsselung

Effektivität der Browserhärtung

Unterschiede in Firefox

Ehrlichkeit

Transparenz

Niklas Baier
niklas.baier@st.ovgu.de

Beurteilung & Zusammenfassung

Niklas Baier
niklas.baier@st.ovgu.de

Ausblick

In dieser Arbeit wurden lediglich die Web Clients von vier viel genutzen E-Mail Anbietern untersucht. Alle Anbieter bieten ebenfalls eigene Apps für mobile Betriebssystem an. Diese sind wesentlich schwieriger datenschutzfreundlich zu konfigurieren und ebenfalls schwerer zu untersuchen. Eine Untersuchung dieser Apps ist Relevant für die Gesamtbeurteilung der Anbieter und für das Erstellen finaler Empfehlungen.

E-Mail Provider werden von nahezu allen Internetnutzern benutzt. Wiederkehrende und u.U. auch automatisierte Untersuchungen wären daher indiziert.

> Jonas Hielscher
> benedikt.hielscher@st.ovgu.de

Literaturverzeichnis

Banday, Tariq. “Analyzing Internet E-Mail Date-Spoofing.” Digital Investigation Journal, 2011. https://www.sciencedirect.com/science/article/pii/S1742287610000812#!