Sicherheit und Privatheit auf deutschen Hochschulwebseiten: Eine Analyse mit PrivacyScore

Tobias Mueller, Dominik Herrmann, Henning Pridöhl,
Matthias Marx, Pascal Wichmann
{mueller,marx,wichmann}@informatik.uni-hamburg.de
{dominik.herrmann,henning.pridoehl}@uni-bamberg.de

Zusammenfassung

Wir untersuchen, inwiefern die Webseiten deutscher Hochschulen gängige Mechanismen zum Schutz von Privatheit und Sicherheit einsetzen. Dazu haben wir 426 Webseiten mit dem Werkzeug *PrivacyScore* analysiert, um u. a. zu ermitteln, ob sie Ressourcen von Drittanbietern einbinden, TLS sicher konfiguriert haben oder bekannte Schwachstellen aufweisen. Wir stellen u. a. fest, dass die Art des Trägers einen messbaren Einfluss auf die Ergebnisse hat und die Umsetzung in den Bundesländern unterschiedlich weit fortgeschritten ist.

1 Einleitung

Der Schutz der Privatsphäre und die Absicherung einer Webseite gegen Angriffe sind Anforderungen, mit denen sich heute grundsätzlich jeder Webseitenbetreiber auseinandersetzen muss. Die korrekte Umsetzung angemessener und wirksamer Mechanismen erfordert Expertise und kontinuierliche Pflege. Ein GroSSteil der Betreiber nutzt (möglicherweise ohne es zu wissen) Tracking-Dienstleister [3], viele Seiten verzichten auf angemessene TLS-Verschlüsselung [14] und bei den meisten fehlen sicherheitsrelevante HTTP-Header [15].

Kommerzielle Anbieter haben kaum Anreize, etwas an dieser Situation zu ändern. Datenschutzfreundliche Umsetzungen verursachen mehr

Arbeit und die Einnahmen aus Tracking und Online-Werbung werden als wichtige Einnahmequelle empfunden [4]. Der Wettbewerb am Markt liefert kaum Anreize zur Verbesserung von Sicherheit und Privatheit. Auch regulatorische Anforderungen laufen bislang weitgehend ins Leere. Häufig wird dort unscharf auf den Stand der Technik verwiesen, allerdings mit der Einschränkung, dass Betreiber nur die ihnen zumutbaren Mechanismen umsetzen müssen.

Bisherige Untersuchungen zur Umsetzung von Sicherheits- und PrivatheitsmaSSnahmen betrachten in der Regel die populärsten Webseiten, z. B. die Alexa Top 1 000 000 [3, 15]. Es existieren jedoch noch kaum Auswertungen für einzelne Sektoren, in denen sensible Daten verarbeitet werden. Ein solcher Sektor sind Hochschulen, die über ihren Webauftritt zahlreiche Dienste zugänglich machen. Neben elektronischer Prüfungs- und Anwesenheitsverwaltung und der Online-Ausleihe von Büchern (Möglichkeit zur Profilbildung anhand des Leseverhaltens) werden Studierenden und Dozenten auch Kommunikationsdienste angeboten.

Inwiefern Privatheits- und Sicherheitsmechanismen auf den Webseiten von Hochschulen angemessen und wirksam umgesetzt sind, ist bislang nicht bekannt. Hochschulen, die aus öffentlichen Mitteln finanziert werden, sollten im Unterschied zu privat finanzierten Universitäten eigentlich keinen Anlass haben, ihre Benutzer mit Tracking-Diensten zu verfolgen. Weiterhin könnte erwartet werden, dass sich Hochschulen, die im Deutschen Forschungsnetz (DFN) Mitglied sind, über die Umsetzung geeigneter Sicherheitsmechanismen austauschen, sodass dort mit einem höheren Umsetzungsgrad zu rechnen ist.

In diesem Beitrag veröffentlichen wir Ergebnisse zur Beantwortung dieser Fragen. Dazu benutzen wir *PrivacyScore.org*, einen Webdienst, mit dem sich entsprechende Prüfungen automatisiert und wiederkehrend durchführen lassen. Dies ist die erste Veröffentlichung, in der Testergebnisse für einen bestimmten Sektor ausgewertet werden.[1] Dieser Beitrag ist daher auch als Diskussionsgrundlage für die Weiterentwicklung von PrivacyScore gedacht. Langfristig soll der Dienst mit einer Oberfläche zur automatisierten Analyse und Auswertung ausgestattet werden.

[1] Technische Details wurden in [8] erläutert, eine rechtliche Betrachtung findet sich in [9].

Unser Beitrag Wir dokumentieren den Umsetzungsgrad von Mechanismen für Privatheit und Sicherheit auf den Webseiten von 426 deutschen Hochschulen. Dabei differenzieren wir nach Standort und Art einer Hochschule und überprüfen, ob Mitglieder im Deutschen Forschungsnetz (DFN) besser aufgestellt sind als Nichtmitglieder.

In Abschnitt 2 stellen wir PrivacyScore vor. Danach beschreiben wir in Abschnitt 3 den verwendeten Datensatz. In Abschnitt 4 präsentieren wir Ergebnisse, die wir in Abschnitt 5 diskutieren. AbschlieSSend folgen Schlussbemerkungen in Abschnitt 6.

2 Der PrivacyScore-Dienst

PrivacyScore.org ist ein im Juni 2017 gestartetes Web-Portal, mit dem automatisiert überprüft werden kann, ob die Betreiber einer Webseite gängige Mechanismen zum Schutz von Sicherheit und Privatheit einsetzen und korrekt konfiguriert haben. PrivacyScore ist freie Software (GPLv3+). Dadurch lässt sich jederzeit nachvollziehen, wie Testergebnisse zustandekommen. Darüber hinaus ist es möglich, einen eigenen (internen) PrivacyScore-Dienst zu betreiben.

PrivacyScore überprüft u. a. die Unterstützung einer aktuellen TLS-Version bei Web- und Mailservern, das Setzen von sicherheitsrelevanten HTTP-Headern und das Verzichten auf Tracking, insbesondere durch Drittanbieter. Auf kommerziellen Webseiten ist ein solches Tracking (und darüber hinausgehende Techniken wie Fingerprinting) heutzutage gang und gäbe [12, 3]. Sowohl Benutzer, Aufsichtsbehörden, aber auch Konkurrenten haben ein Interesse daran, zu erfahren, wie sehr sich Webseitenbetreiber den Möglichkeiten dieses Trackings oder Fingerprintings bedienen und wie sich die Verwendung über die Zeit entwickelt. Die Analyse gliedert sich derzeit in vier Bereiche (Abb. 1):

- **EncWeb:** Mit dem Werkzeug *testssl.sh* [1] wird die zu überprüfende Webseite hinsichtlich ihrer TLS-Implementation untersucht. TLS gewährleistet die Vertraulichkeit der Daten auf dem Transportweg [2]. Veraltete Versionen erlauben es Angreifern auf dem Transportweg, die Kommunikation mitzulesen [6]. Daher ist die Verwendung einer aktuellen Protokollversion (aktuell TLS 1.2) wichtig. Ferner sollten die Betreiber alle Nutzer standardmäSSig auf die

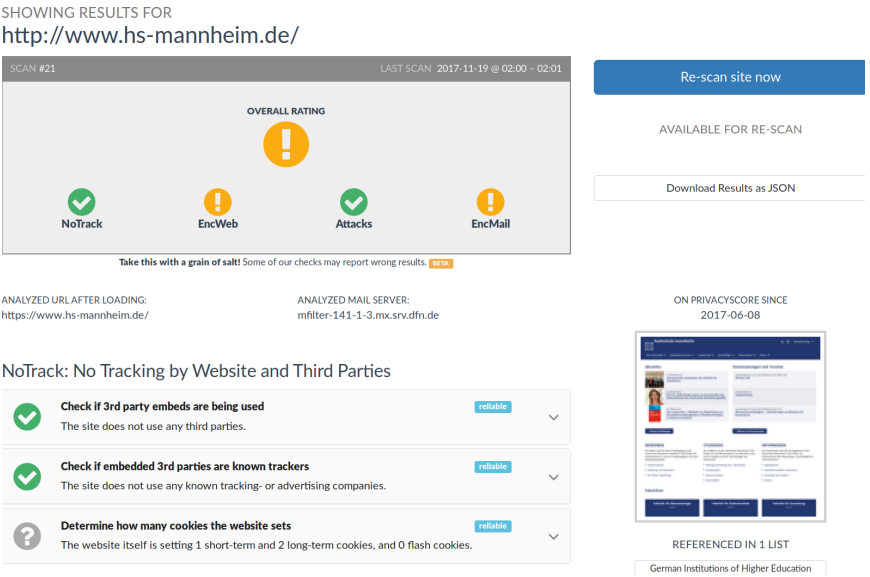

Abbildung 1: Die einzelnen Tests sind in vier Kategorien organisiert. Für jeden Test lassen sich Detailergebnisse anzeigen.

verschlüsselte Webseite umleiten (HTTPS-URL) und den Browser mit dem Strict-Transport-Security-Header dazu anhalten, die HTTPS-Version abzurufen [7]. Dadurch wird nicht nur die Vertraulichkeit geschützt, sondern auch verhindert, dass die ausgetauschten Daten auf dem Transportweg manipuliert werden.

- **EncMail:** Der für eine Domain zuständige Mailserver sollte Transportverschlüsselung mittels des SMTP-Kommandos STARTTLS anbieten [13]. Dies ermöglicht es anderen Mailservern, die Mails über eine verschlüsselte Verbindung einzuliefern und eine Beobachtung auf dem Transportweg zu erschweren. PrivacyScore ermittelt daher die Mailserver, die für eine Webseite zuständig sind (sofern vorhanden) und überprüft die Aktualität und Konfiguration der TLS-Verbindung mit *testssl.sh*.

- **NoTrack:** PrivacyScore ruft jede zu überprüfende Webseite mit dem Werkzeug *OpenWPM* [3] ab. Dabei wird jede Webseite automatisiert mit einem entsprechend instrumentierten Firefox-Browser

heruntergeladen und es wird protokolliert, ob und von welchen Drittanbietern bzw. bekannten Tracking-Dienstleistern Inhalte nachgeladen werden. Weiterhin werden u. a. die Anzahl der Cookies und die Standorte von Web- und Mailserver erfasst.

- **Attacks:** Die Privatsphäre von Nutzern kann auch durch aktive Angriffe beeinträchtigt werden. PrivacyScore untersucht daher zum einen, ob gängige HTTP-Header, etwa *Content-Security-Policy* [17] und *XSS-Protection*, eingesetzt werden. Zum anderen wird überprüft, ob der Webserver aus Unachtsamkeit potenziell sensible Informationen über Konfiguration und eingesetzte Anwendungen preisgibt, etwa weil Datenbank-Dumps und git- oder svn-Repositories ohne Authentifizierung abgerufen werden können.

Vergleich mehrerer Webseiten Das Kernelement von PrivacyScore ist das Anlegen von Listen mit gleichartigen Webseiten wie beispielsweise von Banken, Versicherungen oder Hochschulen. Beim Anlegen einer Liste können jedem Eintrag Attribute hinzugefügt werden. Beispiele für Attribute sind, im Falle von Hochschulen, die Anzahl der Studierenden, das Bundesland oder das Jahr der Gründung. Mit diesen Attributen lassen sich Teilmengen miteinander vergleichen und gegebenenfalls Korrelationen mit den festgestellten Mängeln herstellen.

Die Webseiten einer Liste werden anhand der Ergebnisse in eine Rangfolge gebracht (Abb. 2). Hierzu werden die Seiten zunächst nach den Ergebnissen in den einzelnen Bereichen sortiert, wobei die Reihenfolge der Bereiche durch den Nutzer beeinflusst werden kann. Anschließend werden die Einzelergebnisse der einzelnen Checks aus den Bereichen betrachtet, um die exakte Rangfolge zu bestimmen. Derzeit gibt es 73 Checks, die sich auf die Rangfolge auswirken können.

Im Idealfall schafft die daraus resultierende Transparenz einen zusätzlichen Anreiz für Webseitenbetreiber, sich um den Schutz von Sicherheit und Privatheit zu kümmern. Möglicherweise kommt es sogar zu einem Konkurrenzkampf innerhalb eines Sektors.

PrivacyScore richtet sich nicht nur an datenschutzinteressierte Endanwender, sondern auch an Datenschutz-Aufsichtsbehörden. Diese können mit PrivacyScore mit geringem Aufwand regelmäßig überprüfen, ob diejenigen Organisationen und Unternehmen, die unter ihre Aufsicht fallen, Maßnahmen nach dem Stand der Technik einsetzen und welche

Ranking

#	URL	Name	Land	Traeger	Gruendung	Studierende	AS	NoTrack	EncWeb	Attacks	EncMail	Rating
1	http://www.hs-mannheim.de/ / 2017-11-19 @ 02:01:09	Hochschule Mannheim	BW	staatlich	1898	5106	AS553	✓	!	✓	!	!
2	http://fh-polizei.sachsen-anhalt.de/ / 2017-11-19 @ 07:44:43	Fachhochschule Polizei Sachsen-Anhalt (FPS)	ST	staatlich	1997	316	AS21413	✓	!	!	?	!
3	http://www.archivschule.de/ / 2017-11-19 @ 01:59:58	Archivschule Marburg	HE	staatlich	1949	49	AS45031	✓	!	!	?	!
4	http://www.eh-darmstadt.de/ / 2017-11-19 @ 05:44:02	Evangelische Hochschule Darmstadt	HE	konfessionell	1971	1603	AS8365	✓	!	!	?	!
5	http://www.ph-freiburg.de/ (1 failure) / 2017-11-19 @ 05:12:36	Pädagogische Hochschule Freiburg	BW	staatlich	1962	5067	AS553	✓	!	!	?	!
6	http://www.th-nuernberg.de/ / 2017-11-19 @ 07:21:20	Technische Hochschule Nürnberg Georg Simon Ohm	BY	staatlich	1823	12234	AS680	✓	!	!	?	!
7	http://www.kh-mz.de/ / 2017-11-19 @ 08:28:11	Katholische Hochschule Mainz	RP	konfessionell	1972	1089	AS3320	✓	!	!	?	!

Abbildung 2: Die Webseiten einer Liste werden anhand der Testergebnisse in eine Rangfolge gebracht. Die Nutzer können die Priorität der Kategorien verändern.

MaSSnahmen weit verbreitet sind (und damit zum Stand der Technik gehören).

3 Datensatz

In diesem Abschnitt beschreiben wir, wie wir den Datensatz erhoben haben, den wir in diesem Beitrag verwenden.

Die Basis für den Datensatz ist die Liste der deutschen Hochschulen in der Wikipedia [18]. Dort sind unter anderem das Bundesland, der Träger und die Anzahl der Studierenden hinterlegt. Diese Felder haben wir als Attribute für die Webseiten (vgl. Abschnitt 2) übernommen.

Um die eingangs gestellte Frage nach der Sicherheit und Privatheit von Webseiten von DFN-Mitgliedern beantworten zu können, haben wir die Attribute um die Nummer des Autonomen Systems (AS) [5], in dem die Webseite gehostet ist, erweitert. Mit der AS-Nummer lässt sich herausfinden, ob die Webseite in einem AS des DFN (AS680) gehostet wird. Unter der Annahme, dass diese Dienstleistung nur Mitgliedern zur Verfügung steht, können wir über die AS-Nummer mit verhältnismäSSig wenig Aufwand herausfinden, ob eine Universität Mitglied im DFN ist. Die Methode schlieSSt Webseiten aus, die nicht im AS des DFN gehostet sind. Diesen Fehler nehmen wir in Kauf. Eine korrektere Möglichkeit, DFN-Mitglieder zu bestimmen, ist die vom DFN angebotene Mitglie-

Tabelle 1: Beispiel-Eintrag aus der Liste der Hochschulen

Attribut	Beschreibung	Wert
Hochschule	Bezeichnung	Universität Hamburg
URL	überprüfte Webseite	*http://www.uni-hamburg.de*
Land	eines der 16 Bundesländer	HH
Träger	staatlich, privat, konfessionell	staatlich
Promotionsrecht	ja/nein	ja
Gründung	Jahreszahl	1919
Studierende	Anzahl der Studierenden	42023
AS	Autonomes System	AS680
Stand	Jahreszahl	2015/16 (WS)

derliste (https://www.dfn.de/verein/mv/mitglieder/). Diese war jedoch für uns nicht einfach zu konsumieren, denn die Namen und Adressen der Webseiten hätten mit manuellem Aufwand mit denen der Wikipedia abgestimmt werden müssen.

Um die Vollständigkeit unseres Datensatzes zu validieren, haben wir die Anzahl der Studierenden mit den Zahlen des Statistischen Bundesamtes (2 757 799 im Jahr 2015) verglichen [16]. Unser Wert ist 8 % niedriger. Dieser Unterschied erklärt sich zum einen durch den zeitlichen Abstand sowie unterschiedliche Erhebungsmethoden. Wir haben die Korrektheit der Einträge nicht gesondert überprüft und verlassen uns auf die QualitätssicherungsmaSSnahmen der Wikipedia. Die resultierende Liste enthält 426 Hochschulen (https://privacyscore.org/list/87/). Zur Veranschaulichung ist ein Eintrag der Liste in Tabelle 1 dargestellt.

4 Ergebnisse

Wir haben den im vorigen Abschnitt beschriebenen Datensatz mit PrivacyScore analysiert. In diesem Abschnitt stellen wir unsere Ergebnisse vor.

4.1 Einfluss der Trägerschaft

Zunächst betrachten wir, inwiefern die Art der Trägerschaft Einfluss auf die Tests der Kategorie **NoTrack** hat. Zu dieser Kategorie gehören Tests, mit denen u. a. untersucht wird, ob Webseiten Dienste von Drittanbie-

Tabelle 2: Anteil der Seiten mit *gutem* Gesamtergebnis in der Kategorie **NoTrack**. Gute Seiten setzen keine Tracking-Dienste von Drittanbietern ein und ihre Web- und Mailserver sind in der EU.

	konfessionell	privat	staatlich	(Summe)
Seiten	43	110	269	422
NoTrack *gut*	23 %	3 %	48 %	33 %

Tabelle 3: Anteil der Seiten mit *schlechtem* Gesamtergebnis in der Kategorie **EncWeb**. Schlechte Seiten bieten kein HTTPS, weisen Fehlkonfigurationen auf oder es erfolgt keine Weiterleitung zu HTTPS.

	konfessionell	privat	staatlich	(Summe)
Seiten	43	110	269	422
schlecht	65 %	55 %	67 %	64 %

tern einbinden, die zum Tracking von Nutzern dienen. Darüber hinaus wird durch Nachschlagen in der GeoIP-Datenbank von MaxMind [11] überprüft, ob sich Web- und Mailserver in einem Land der EU befinden.

Die Ergebnisse dieser Analyse sind in Tabelle 2 dargestellt. Hochschulen unter konfessioneller und staatlicher Trägerschaft schneiden dabei deutlich besser ab als solche, die privat finanziert werden. Dennoch überrascht es, dass auch bei staatlich finanzierten Hochschulen mehr als die Hälfte der untersuchten Webseiten Dienste von Drittanbietern (häufig aus den USA) in Anspruch nimmt.

Als nächstes betrachten wir die Kategorie **EncWeb**. Hier geht es v. a. um das Vorhandensein und die Qualität der Transportverschlüsselung (HTTPS). Die Ergebnisse sind in Tabelle 3 dargestellt. In dieser Kategorie spielt die Trägerschaft nur eine untergeordnete Rolle. Fast zwei Drittel der Seiten schneiden hier schlecht ab.

Deutlich weiter fortgeschritten ist die Umsetzung der Transportverschlüsselung bei den Mailservern. Die Ergebnisse für die Kategorie **EncMail** sind in Tabelle 4 dargestellt. Mehr als 90 % der Hochschulen nehmen demnach Mails über TLS-Verbindungen entgegen. Staatlich finanzierte Hochschulen schneiden in dieser Kategorie etwas schlechter ab als konfessionell oder privat getragene Hochschulen.

Tabelle 4: Anteil der Seiten mit *schlechtem* Gesamtergebnis in der Kategorie **EncMail** (nur Seiten mit Mailserver). Die Mailserver schlechter Seiten bieten kein TLS an oder es liegen Konfigurationsfehler vor.

	konfessionell	privat	staatlich	(Summe)
Seiten	32	97	186	315
schlecht	6 %	6 %	11 %	8 %

Tabelle 5: Anzahl der Webseiten mit unterschiedlichen Ergebnissen in den Kategorien EncWeb und EncMail. Es werden nur Seiten betrachtet, bei denen die Tests in beiden Kategorien fehlerfrei durchgelaufen sind.

	EncWeb *schlecht*	EncWeb *akzeptabel*	Summe
EncMail *schlecht*	14	14	28
EncMail *akzeptabel*	179	103	282
Summe	193	117	310

Die beobachtete Diskrepanz von Mailservern mit Transportverschlüsselung zu Webservern lässt sich dadurch erklären, dass die Aktivierung von STARTTLS wesentlich weniger Aufwand macht als die Absicherung eines Webservers. Die Tatsache, dass eine Hochschule in der Kategorie EncMail gut abschneidet, bedeutet daher nicht, dass sie auch in EncWeb ein gutes Ergebnis erzielt (Tabelle 5). Allerdings gibt es auch keinen umgekehrten Zusammenhang: Nicht alle Hochschulen, die einen gut abgesicherten Webserver betreiben, betreiben auch einen gut abgesicherten Mailserver.

4.2 Einfluss von Promotionsrecht und DFN-Mitgliedschaft

In diesem Abschnitt betrachten wir zwei weitere Attribute, zum einen ob eine Hochschule das Promotionsrecht hat, zum anderen ob sie über das Deutsche Forschungsnetz angebunden ist.

Zunächst wird die Teilmenge der **152 Hochschulen mit Promotionsrecht** betrachtet. In dieser Teilmenge haben 67 % ein *schlechtes* Ergebnis in der Kategorie **EncWeb**. Bei den 274 Hochschulen ohne Pro-

motionsrecht ist dieser Anteilswert etwas geringer (60 %). Bei **EncMail** betragen die Anteilswerte 8,5 % bzw. 5,5 %. Stärkere Abweichungen gibt es in der Kategorie **NoTrack**: Ein *gutes* Ergebnis erzielen hier 49 % der Hochschulen mit Promotionsrecht, jedoch lediglich 23 % der Hochschulen ohne Promotionsrecht.

Nun betrachten wir die Teilmenge der **149 Hochschulen im Deutschen Forschungsnetz** (Zugang über AS680). In dieser Teilmenge haben 63 % ein *schlechtes* Ergebnis in der Kategorie **EncWeb**. Bei den 277 übrigen Hochschulen ist dieser Anteilswert nahezu gleich hoch (62 %). Bei **EncMail** betragen die Anteilswerte 6,7 % bzw. 6,5 %. Stärkere Abweichungen ergeben sich wieder in der Kategorie **NoTrack**: Ein *gutes* Ergebnis erzielen hier 51 % der Hochschulen im DFN, jedoch erneut lediglich 23 % der übrigen Hochschulen.

4.3 Regionale Unterschiede

Mit unserem Datensatz lassen sich auch regionale Unterschiede aufzeigen. Für die Kategorien EncWeb und NoTrack haben wir eine überblicksartige Auswertung durchgeführt. Demnach gibt es erhebliche Unterschiede beim Grad der Umsetzung der Transportverschlüsselung auf Webservern und der Inanspruchnahme von Drittanbietern auf den Webseiten (Abb. 3).

In der Kategorie **EncWeb** ist der Anteil der Hochschulen mit einem *schlechten Ergebnis* in den Bundesländern Mecklenburg-Vorpommern (100 %), Saarland (83 %) und Sachsen (75 %) am höchsten. Die Bundesländer mit dem niedrigsten Anteil sind Niedersachsen (43 %), Rheinland-Pfalz (58 %) und Hessen (59 %).

In der Kategorie **NoTrack** ist der Anteil der Hochschulen mit einem *guten Ergebnis* hingegen in den Bundesländern Mecklenburg-Vorpommern (100 %), Rheinland-Pfalz (79 %) und Sachsen-Anhalt (75 %) am höchsten. Die Schlusslichter sind hier Berlin (19 %), Hamburg (32 %) und Nordrhein-Westfalen (34 %).

4.4 Weitere Auswertungen

Um Besucher einer Internetseite vor Man-in-the-Middle-Angriffen zu schützen, reicht es nicht aus, HTTPS korrekt zu konfigurieren und eine aktuelle TLS-Protokollversion anzubieten. Eine zusätzliche Sicherheits-

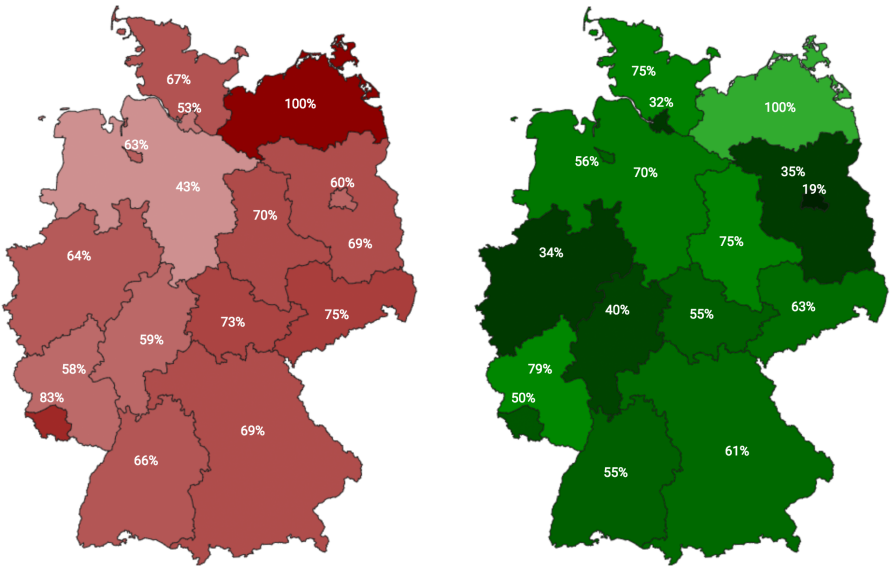

Abbildung 3: Anteil der Webseiten mit *schlechtem* Gesamtergebnis bei EncWeb (links, höherer Anteil ist *schlechter*) bzw. mit *gutem* Gesamtergebnis in der Kategorie NoTrack (rechts, höherer Anteil ist *besser*).

maSSnahme ist das Senden eines geeigneten Strict-Transport-Security-Headers (HSTS) (vgl. Abschnitt 2). Bei unseren Untersuchungen setzten nur 56 Webseiten (13 %) diesen HTTP-Header. Hier herrscht noch erheblicher Nachholbedarf. Im Vergleich mit den Seiten in der Alexa Top 1 000 000 ist dieser Anteilswert allerdings gut (dort: 7 % [15]).

Einer unserer Tests in der Attacks-Kategorie überprüft, ob eine Webseite unabsichtlich sensible Informationen über ihre Konfiguration oder die eingesetzte Software einsetzt. Diese Informationen können Angreifern das Eindringen in einen Server und schlimmstenfalls den Zugriff auf sensible Daten erleichtern. PrivacyScore versucht daher u. a. *phpinfo.php*, *test.php*, */server-status/*, */.git/*, */.svn/* und vergessene Datenbank-Sicherungen an häufig verwendeten Orten von dem zu überprüfenden Webserver herunterzuladen. Zum Zeitpunkt der Fertigstellung des Manuskripts wurden wir dabei auf 23 Webseiten (5,4 %) fündig.

5 Diskussion

Im Folgenden diskutieren wir die Aussagekraft der Ergebnisse. Zunächst ist festzuhalten, dass es sich bei den betrachteten Webseiten um die Startseiten der Hochschulen handelt. Diese Seiten dienen üblicherweise als Einstiegspunkt und nicht der Erfassung sensibler Daten. Zur Klärung der tatsächlichen Sicherheit sind unsere Auswertungen daher nicht geeignet. Hierzu müssten andere URLs betrachtet werden (z. B. Single-Sign-On-URLs oder Webseiten der Studienverwaltungssysteme[2]). Die Betrachtung der Startseiten ist dennoch von Interesse, da sie Interessenten, Studierenden und Mitarbeitern häufig als Einstiegspunkt dienen. Die Einbindung externer Tracking-Dienste auf den Startseiten ist daher ebenso problematisch wie das Fehlen von Transportverschlüsselung. Fehlen Mechanismen wie HSTS zur Verhinderung von Man-in-the-Middle-Angriffen können Angreifer unter bestimmten Umständen SSL-Stripping-Angriffe [10]) durchführen oder Nutzer unbemerkt auf eine Phishing-Seite umleiten.

Zweitens stammen die von uns untersuchten Attribute der Hochschulen aus der Wikipedia, da diese verhältnismäSSig einfach zu verwerten waren. Dadurch konzentrierten sich unsere Untersuchungen auf eben diese Attribute. Unsere Ergebnisse offenbaren beispielsweise einen Unterschied zwischen Universitäten mit und ohne Promotionsrecht (schneiden bei NoTrack vergleichsweise schlecht ab). Die Ursachen für diese Diskrepanz haben wir nicht abschlieSSend untersucht. So könnte man vermuten, dass Hochschulen ohne Promotionsrecht intensiveres Online-Marketing betreiben, um Studieninteressierte auf sich aufmerksam zu machen.

AbschlieSSend sei darauf hingewiesen, dass die Scan-Ergebnisse nicht von Hand verifiziert worden sind. Es kann daher nicht ausgeschlossen werden, dass die Ergebnisse durch temporäre oder systematische Scan-Fehler verzerrt sind. PrivacyScore befindet sich derzeit noch im Beta-Test und wird laufend weiterentwickelt. Es kann dabei zu erheblichen Änderungen im Ranking kommen. Die dargestellten Auswertungen basieren auf Ergebnissen, die am 14. September 2017 erhoben worden sind (Ergebnisse für die zehn am besten abschneidenden Seiten finden sich

[2] Liste mit LSF-Login-Seiten einiger Universitäten: https://privacyscore.org/list/43

im Anhang). Zu Abweichungen kann es auch durch zwischenzeitliche Änderungen an den Webseiten kommen. Die unter https://privacyscore.org/list/87/ dargestellten Ergebnisse stimmen daher nicht mit den hier publizierten Ergebnissen überein.

6 Schlussbemerkungen

In diesem Beitrag haben wir erste Ergebnisse unserer Analyse der Webseiten deutscher Hochschulen vorgestellt. Demzufolge wird von den meisten Mailservern bereits eine Transportverschlüsselung unterstützt, die dem Stand der Technik entspricht. Wesentlich schlechter fallen die Ergebnisse für Webserver aus. Weniger als die Hälfte der betrachteten Homepages erfüllt die Mindestvoraussetzungen zum Schutz vor Man-in-the-Middle-Angriffen. Überraschend ist auch die groSSe Zahl der Seiten, die externe Tracking-Dienstleister einbinden und dadurch häufig vermutlich unnötigerweise Informationen über das Nutzungsverhalten ihrer Studierenden und Mitarbeiter an ausländische Anbieter weitergeben.

Die Ergebnisse in diesem Beitrag sind naturgemäSS schon zum Zeitpunkt der Veröffentlichung veraltet. Da wir für unsere Analyse den Online-Dienst PrivacyScore benutzt haben, können jedoch laufend aktualisierte Ergebnisse online eingesehen werden. Die Auswertungen, die wir in diesem Beitrag von Hand durchgeführt haben, werden wir schrittweise in PrivacyScore integrieren. Geplant sind darüber hinaus Mechanismen zur Durchführung von Längsschnitt-Studien, um Veränderungen im Zeitverlauf erkennen zu können. Die dafür nötigen Daten werden von PrivacyScore bereits kontinuierlich gesammelt.

Wir hoffen, dass die Veröffentlichung dieses Beitrags dazu führt, dass die Hochschulrechenzentren ihre Infrastruktur überprüfen und darauf hinwirken, dass Sicherheit und Privatheit ihrer Besucher verbessert werden.

Literatur

[1] D. Wetter: testssl.sh (2017), https://testssl.sh/

[2] Dierks, T., Rescorla, E.: The transport layer security (TLS) protocol version 1.2, https://tools.ietf.org/html/rfc5246

[3] Englehardt, S., Narayanan, A.: Online tracking: A 1-million-site measurement and analysis. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS 2016). pp. 1388–1401. ACM (2016)

[4] Goldfarb, A., Tucker, C.E.: Privacy regulation and online advertising. Management Science 57(1), 57–71 (2011), https://doi.org/10.1287/mnsc.1100.1246

[5] Hawkinson, J., Bates, T.: Guidelines for creation, selection, and registration of an autonomous system (AS), https://tools.ietf.org/html/rfc1930

[6] Holz, R., Sheffer, Y., Saint-Andre, P.: Summarizing known attacks on transport layer security (TLS) and datagram TLS (DTLS), https://tools.ietf.org/html/rfc7457

[7] Jackson, C., Barth, A., Hodges, J.: HTTP strict transport security (HSTS), https://tools.ietf.org/html/rfc6797

[8] Maass, M., Herrmann, D.: PrivacyScore: Improving Privacy and Security via Crowd-Sourced Benchmarks of Websites. In: Schweighofer, E., Leitold, H., Mitrakas, A., Rannenberg, K. (eds.) Privacy Technologies and Policy - 5th Annual Privacy Forum, APF 2017, Vienna, Austria, June 7-8, 2017, Revised Selected Papers. Preprint: https://arxiv.org/abs/1705.05139. pp. 178–191. No. 10518 in Lecture Notes in Computer Science, Springer (2017)

[9] Maass, M., Laubach, A., Herrmann, D.: PrivacyScore: Analyse von Webseiten auf Sicherheits- und Privatheitsprobleme – Konzept und rechtliche Zulässigkeit. In: Eibl, M., Gaedke, M. (eds.) INFORMATIK 2017. Preprint: https://arxiv.org/abs/1705.08889. pp. 1049–1060. Gesellschaft für Informatik, Bonn (2017)

[10] Marlinspike, M.: New Tricks For Defeating SSL In Practice, BlackHat USA (2009), http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf

[11] MaxMind: GeoLite2 Free Downloadable Databases (2017), https://dev.maxmind.com/geoip/geoip2/geolite2/

[12] Mayer, J.R., Mitchell, J.C.: Third-party web tracking: Policy and technology. In: 2012 IEEE Symposium on Security and Privacy. pp. 413–427

[13] Newman, C.: Using TLS with IMAP, POP3 and ACAP, https://tools.ietf.org/html/rfc2595

[14] Qualys: SSL Pulse (2017), https://www.ssllabs.com/ssl-pulse/

[15] S. Helme: Alexa Top 1 Million Analysis - August 2017 (2017), https://scotthelme.co.uk/alexa-top-1-million-analysis-aug-2017/

[16] Statistisches Bundesamt: Zahlen & Fakten: Studierende (2017), https://www.destatis.de/DE/ZahlenFakten/Indikatoren/LangeReihen/Bildung/lrbil01.html

[17] West, M.: Content security policy level 3, https://www.w3.org/TR/CSP/

[18] Wikipedia: Liste der Hochschulen in Deutschland (2017), https://de.wikipedia.org/wiki/Liste_der_Hochschulen_in_Deutschland

A Betrachtete Webseiten

Die folgende Aufstellung enthält die 12 bestplatzierten betrachteten Webseiten nach dem PrivacyScore-Ranking (Stand 19.11.2017).

Rang	Webseite	DFN-Mitgliedschaft
1	www.hs-mannheim.de	nein
2	fh-polizei.sachsen-anhalt.de	nein
3	www.archivschule.de	nein
4	www.eh-darmstadt.de	nein
5	www.ph-freiburg.de	nein
6	www.th-nuernberg.de	ja
7	www.kh-mz.de	nein
8	www.uni-marburg.de	ja
8	www.hs-wismar.de	ja
9	www.fh-bielefeld.de	ja
9	www.reutlingen-university.de	nein
10	www.hs-flensburg.de	ja

All diese Webseiten erfüllen die folgenden Kriterien:

- Es werden keine Third-Party-Requests genutzt
- Die Webserver stehen in der EU
- Es wird HTTPS angeboten und HTTP-Anfragen dorthin umgeleitet
- Veraltete SSL-Versionen, die bekannt unsicher sind, werden nicht angeboten
- Die Server sind nicht für bekannte TLS-Angriffe anfällig
- Es konnten keine Leaks gefunden werden

Die bestplatzierte Seite www.hs-mannheim.de nutzt zudem HTTP Strict Transport Security, um den Abruf der Seite über gesicherte HTTPS-Verbindungen zu erzwingen.

Von den Seiten werden allerdings folgende Schutzmechanismen überwiegend nicht genutzt:

- HTTP-Header zum Schutz vor Cross-Site-Scripting-Angriffen
- Mit Ausnahme der Seite auf Rang 10 nutzt keine der aufgeführten Seiten einen Header zur Beeinflussung der Referrer-Policy, um die Privatheit der Nutzer zu steigern
- HTTP Strict Transport Security Preloading zum Erzwingen von HTTPS-Verbindungen auf Browser-Ebene