HOCHSCHULE HANNOVER
UNIVERSITY OF APPLIED SCIENCES AND ARTS
Fakultät IV

ALTHAMMER & KILL

Studie zur Sicherheit von Web-Servern in der Sozialwirtschaft

Untersuchung von Web-Servern führender Sozialunternehmen auf
- *Nutzung von Verschlüsselungsverfahren per https*
- *Schwachstellen beim Einsatz von SSL/TLS*
- *Berücksichtigung gesetzlicher Vorgaben*

von Prof. Dr.-Ing. Peter Merz
und Thomas Althammer

Hannover, Dezember 2016

Abstract

Die neuen Medien haben in der Sozialwirtschaft Einzug gehalten: Immer mehr Menschen informieren sich online über Träger, Einrichtungen und Dienste. Moderne Instrumente der Marktkommunikation sind eine wichtige Säule im Kontakt mit Kunden, Mitarbeitenden, Medien, aber auch Ehrenamtlichen und Förderern.

Für die Übermittlung personenbezogener Daten ist eine verschlüsselte Übertragung unverzichtbar und seit Jahren etabliert. Durch die erhöhte Datenschutz-Sensibilität gewinnt der vertrauliche Zugriff über https auf die Websites von Sozialunternehmen an Bedeutung. Sobald über Kontaktformulare oder etwa Bewerberportale der Austausch personenbezogener Daten angeboten wird, ist mit Einführung des IT-Sicherheitsgesetzes im Juli 2015 eine SSL-Verschlüsselung zur Pflicht geworden.

Die nachfolgende Studie beleuchtet den aktuellen Umsetzungsgrad zur Sicherheit von Web-Server in der Sozialwirtschaft. Es wird dargestellt, in welchem Umfang heute https-basierte Zugriffe auf die Internetseiten von Sozialunternehmen möglich sind. Darüber hinaus werden mögliche Probleme in der technischen Implementierung überprüft und ausgewertet.

Kontakt

HOCHSCHULE HANNOVER
UNIVERSITY OF APPLIED SCIENCES AND ARTS
Fakultät IV Wirtschaft und Informatik

Peter Merz
Professor für Wirtschaftsinformatik, insbes. Informationssicherheit
Hochschule Hannover
Fakultät IV- Wirtschaft und Informatik
Ricklinger Stadtweg 120
30459 Hannover
peter.merz@hs-hannover.de

ALTHAMMER & KILL

Thomas Althammer
Geschäftsführer
Althammer & Kill GmbH & Co. KG
Standort Hannover
Buchenhain 15
30938 Burgwedel
ta@althammer-kill.de

Bedeutung der Web-Sicherheit

Die Web-Präsenz einer Organisation ist Aushängeschild im Internet und längst für nahezu alle Organisationen unverzichtbar. Das Internet spielt für Sozialunternehmen eine wichtige Rolle in der Kommunikation nach außen, beim Personalmarketing oder etwa dem Belegungsmanagement. Deshalb sollten die Verfügbarkeit des Web-Servers und die Integrität der auf dem Server gespeicherten und zur Verfügung gestellten Daten jederzeit gewährleistet sein.

Bei Unternehmen, bei denen der Web-Server innerhalb des eigenen IT-Netzes betrieben wird, kann der Web-Server als eine für alle Internet-Teilnehmer sichtbare Eingangstür in das Unternehmensnetz angesehen werden. Dass diese Tür einen guten Schutzmechanismus benötigt, liegt auf der Hand. Ein potenzieller Angreifer wird zudem von der (Un-)Sicherheit des oder der Web-Server auf die (Un-)Sicherheit des gesamten IT-Netzes schließen: Werden beispielsweise die Software auf einem Web-Server nicht aktualisiert und Sicherheitslücken nicht behoben, so wird dies wahrscheinlich auch bei anderen IT-Komponenten der Fall sein.

So gesehen stellt die Sicherheit des Web-Servers einen Indikator für ein funktionierendes Sicherheitsmanagement im Unternehmen dar. Die durchgeführte Studie erlaubt also in Grenzen Rückschlüsse von der Web-Server-Sicherheit auf die Sicherheit des gesamten IT-Verbundes und damit auf das Vorhandensein eines funktionierenden IT-Sicherheitsmanagements.

Relevanz und rechtliche Grundlagen

Sozialunternehmen verarbeiten teils äußerst sensible personenbezogene Daten, für die ein hoher Schutzbedarf besteht. Werden solche Daten über die Web-Präsenz der Organisation ausgetauscht, müssen insbesondere Schutzmaßnahmen nach dem Stand der Technik getroffen werden, um die Integrität und Vertraulichkeit der übermittelten Daten sicherstellen.

Nach dem Telemediengesetz (TMG) ist die Übermittlung von personenbezogenen Daten entsprechend dem Stand der Technik zu sichern (vgl. § 13 Abs. 7 Nr. 2). Auf den Internet-Seiten der Unternehmen sind vielfach Kontaktformulare ein Einsatz, häufig auch weitergehende Anwendungen wie z. B. ein Bewerbungsportal. Existiert hier keine oder eine fehlerhaft implementierte Verschlüsselung, ist eine Sicherung der personenbezogenen Daten der Website-Besucher nicht gewährleistet.

Als anerkannter Stand der Technik bei der Nutzung von Angeboten im Internet gilt der Einsatz von Zertifikats-basierten Verschlüsselungsverfahren per SSL/TLS. Ein sicherer Zugriff schafft Vertrauen, der durch eine Client-seitige Überprüfung in den gängigen Web-Browser verifiziert und entsprechend gekennzeichnet wird.

Hersteller von Internet-Browsern haben angekündigt, in Zukunft vermehrt bei Besuch unverschlüsselter Websites zu warnen. Der Einsatz von SSL/TLS auf einer Website wirkt sich positiv auf das Ranking bei Suchmaschinen aus.

Methoden zur Überprüfung der Sicherheit von Web-Servern

Für die Überprüfung von IT-Systemen über das Netzwerk bzw. das Internet gibt es viele verschiedene Werkzeuge. Ein häufig eingesetztes Werkzeug ist der Port-Scanner, der alle aus dem Internet erreichbaren Dienste bzw. Ports ausfindig macht. Für die einzelnen Dienste wie z.B. Web-Server, E-Mail-Server oder Netzwerkfreigabe gibt es spezielle Werkzeuge, die nach Schwachstellen suchen oder sie ausnutzen. Auch existieren umfangreiche, allgemeine Schwachstellen-Suchwerkzeuge (*Vulnerabilty scanner*) und Werkzeuge zum Ausnutzen (*Exploit*) von Schwachstellen.

Für Web-Server gibt es spezialisierte Tools, die Schwachstellen in der Konfiguration oder in der Software selbst finden, sowie Tools, die Schwachstellen in Content Management Systemen aufdecken. Viele der Werkzeuge sind frei verfügbar und stehen Angreifen wie IT-Sicherheitsprüfern (Penetrationstestern) gleichermaßen zur Verfügung.

Auch gibt es Suchmaschinen, wie www.shodan.io, die es ermöglichen, nach speziellen Diensten im Internet bis hin zu Schwachstellen zu suchen. So lassen sich z.B. ungeschützte Internetzugänge von Industrieanlagen ausfindig machen.

In der Studie angewandte Methoden

IT-Sicherheitsüberprüfungen dürfen im Allgemeinen nur mit Erlaubnis des überprüften Unternehmens durchgeführt werden; z.B. dann, wenn Schwachstellen nicht nur aufgedeckt, sondern auch ausgenutzt werden. Selbst einfachere Überprüfungen wie Port-Scans sind u.U. nicht zulässig, da diese Überprüfungen die untersuchten Systeme und Netzwerke unter Last stellen.

Daher wurde hier von solchen Prüfungen abgesehen und nur einfache Prüfungen, die im Zuge eines einfachen Web-Seiten-Abruf erfolgen, durchgeführt. Ein Beispiel hierfür ist die Überprüfung der von Web-Servern übermittelten Versionsnummern der eingesetzten Software: Bei dem Abruf einer Webseite antwortet der Web-Server wie folgt bevor der eigentliche Inhalt der Web-Seite übertragen wird:

```
HTTP/1.1 200 OK
Date: Thu, 17 Mar 2016 08:40:30 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u2
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```

In diesem HTTP-Header sind die Versionsnummern des Apache-Web-Servers sowie der PHP-Engine (in Rot dargestellt) enthalten. Anhand der Versionsnummern lässt sich nun u.U. ermitteln, wie alt die eingesetzte Software ist und ob sie bekannte Schwachstellen enthält.

Da nicht alle Server diese Versionsnummern übertragen und man nicht immer auf mögliche Schwachstellen schließen kann, wurde eine weitere Überprüfung durchgeführt. Während des

Verbindungsaufbaus mit einem Web-Server, der Verschlüsselung unterstützt, kann ermittelt werden, ob die verwendete Verschlüsselungssoftware (SSL) Schwachstellen enthält, ohne dass diese ausgenutzt oder der Server in einer anderen Form in seiner Funktion beeinträchtigt wird.

In der Studie wurden vier Schwachstellen in SSL betrachtet, die in Tabelle 1 dargestellt sind.

Kennung	Name	Geschlossen seit:
CVE-2014-0160	OpenSSL „Heartbleed“ Schwachstelle	April 2014
CVE-2014-0224	„CCS Injection" Schwachstelle	Juni 2014
CVE-2014-3566	SSLv3 Schwachstelle “Poodle”	Oktober 2014
CVE 2015-4000	DiffieHellman-Schwachstelle “logjam”	Mai 2015

Tabelle 1: SSL-Schwachstellen

Mit Hilfe der Kennung können zu den einzelnen Schwachstellen ausführliche Informationen unter http://www.cvedetails.com/ abgerufen werden. Es handelt sich um Schwachstellen mit hohem Bekanntheitsgrad, die in 2014 bzw. 2015 geschlossen wurden. Als Werkzeug zur Überprüfung wurde *nmap* eingesetzt, welches in der Lage ist, gezielt und ausschließlich nach den vier Schwachstellen zu suchen ohne den Server zu beeinträchtigen (*nmap script category: safe*).

Untersuchte Organisationen

Insgesamt wurden 193 Organisationen aus dem Bereich des Sozialwesens betrachtet. Es handelt sich hierbei um die größten freigemeinnützigen Sozialunternehmen in Deutschland, jeweils bezogen auf die Regionen Nord, Ost, West und Süd. Grundlage war eine entsprechende Veröffentlichung der Zeitschrift Wohlfahrt Intern in der Ausgabe 09/2015.

Die untersuchten Organisationen gehören zu den Spitzenverbänden der Freien Wohlfahrtspflege von Arbeiterwohlfahrt (AWO), dem Deutschen Caritasverband (Caritas), dem Paritätischen Wohlfahrtsverband (der Paritätische), dem Deutschen Roten Kreuz (DRK) und der Diakonie Deutschland (Diakonie). Nach Angaben des veröffentlichten Rankings erwirtschaften sie insgesamt einen Umsatz von rund 28 Milliarden Euro.

Die 193 Organisationen haben ihre Web-Präsenzen auf 188 verschiedenen Web-Servern. Das liegt daran, dass einige Träger für ihre Organisationen hosten.

Ergebnisse der Studie

Zunächst wurde allgemein ermittelt, welche Web-Server-Implementationen eingesetzt werden (vgl. Abbildung 1). Mit 86,0% ist Apache der am häufigsten eingesetzte Web-Server. Microsoft IIS hat nur einen Anteil von 2.7%. Welche Versionen von Apache eingesetzt werden, lässt sich nur zum Teil ermitteln, da 54.9% der Server die Versionsnummer nicht in HTTP-Anfragen mitteilen. Anhand der Versionsnummer ist es in einigen Fällen schwer, auf enthaltene Schwachstellen zu schließen, da im Zuge des Long-Term-Supports sicherheitsrelevante *Patches* (Fehlerbereinigungen) in ältere Versionen eingefügt werden (sogenannte *backports*).

Ein Beispiel ist Apache 2.2. Die aktuelle Version war zur Zeit der Durchführung der Studie ist 2.2.31. Einige Linux-Distributionen verwenden aber noch Version 2.2.22, die aber die alle sicherheitsrelevanten Änderungen von Version 2.2.31 beinhalten.

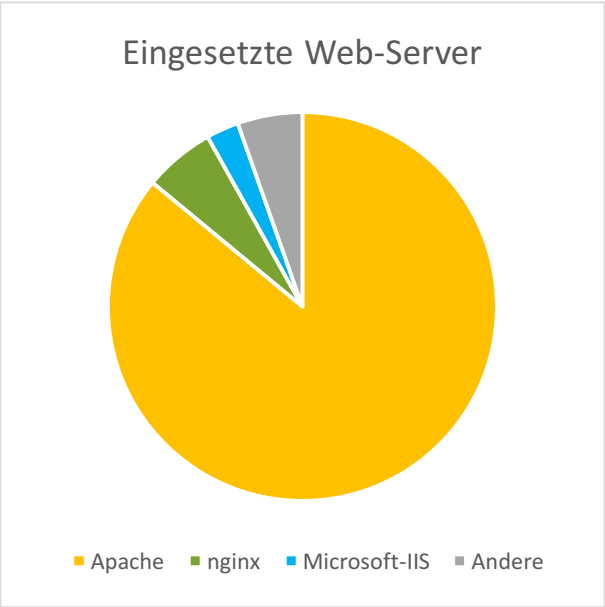

Abbildung 1: HTTP-Server

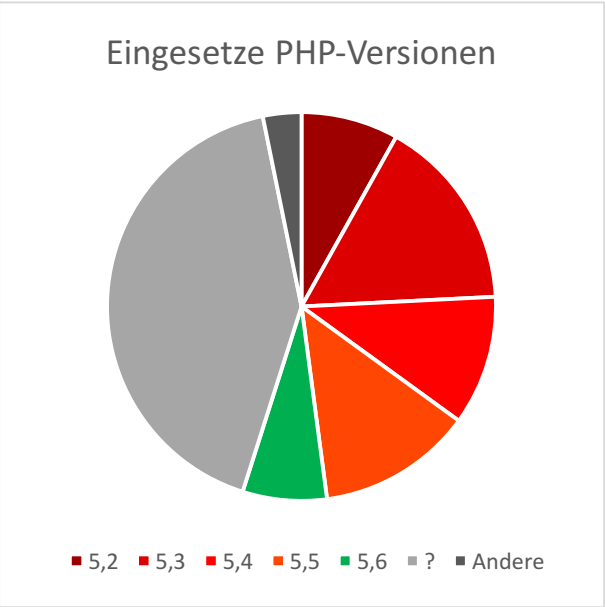

Abbildung 2: PHP-Versionen

Die Betrachtung der eingesetzten PHP-Versionen liefert ein ähnliches Bild, wie in Abbildung 2 dargestellt. Auch hier werden die Versionsnummern nur von einem Teil der Web-Server übertragen: 109 von 188 HTTP-Servern geben diese Information preis.

Insgesamt verwenden mindestens 47.9% der Server PHP in einer Version kleiner als Version 5.6. Über eine große Zahl der Server (in der Grafik grau dargestellt) lässt sich keine Aussage treffen. Diese Zahlen lassen einen großen Anteil an veralteter Softwareversionen mit möglichen Schwachstellen vermuten, da alle PHP-Versionen kleiner 5.6 ihren End-of-Life-Status erreicht haben und nicht mehr weiter gepflegt werden.

Die PHP-Entwickler raten ein Upgrade auf höhere Versionen durchzuführen. Abbildung 3 zeigt die Support-Spannen der einzelnen PHP-Versionen.

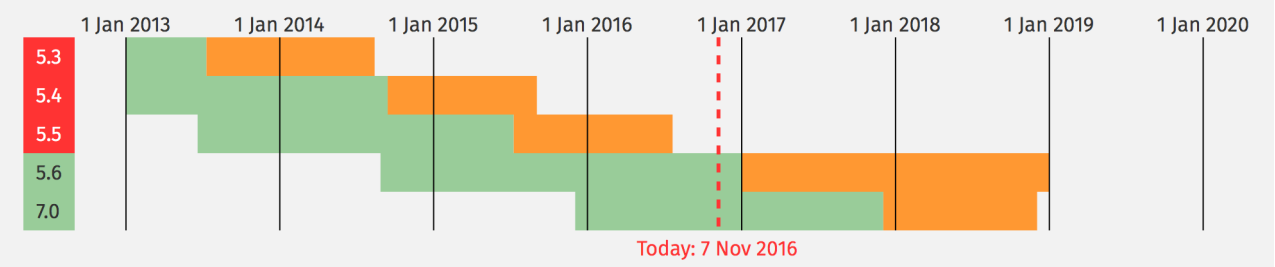

Abbildung 3: PHP-Lebenszyklen (Quelle: http://php.net/supported-versions.php)

Auch hier können *Backports* von Patches die Aussagekraft der Versionsnummer beeinflussen, daher wurde auf eine zweite Methode zur Ermittlung der Softwareaktualität zurückgegriffen: Die Untersuchung auf Schwachstellen in der verwendeten SSL-Verschlüsselungsimplementierung.

Wie oben beschrieben, wurde nach vier SSL-Schwachstellen gesucht. Dies ist nur möglich bei Web-Servern, die überhaupt verschlüsselte Verbindungen unterstützen. Dies sollte bei Unternehmensservern der Fall sein, da nur so die Authentizität des Servers gewährleistet ist und die Kommunikation nicht abgehört oder manipuliert werden kann.

Die Untersuchung ergab, dass von 188 Web-Servern 44 Web-Server keine verschlüsselten Verbindungen anbieten, wie in Abbildung 4 dargestellt. Von den verbleibenden Web-Servern mit Verschlüsselung enthalten 24,3% Schwachstellen.

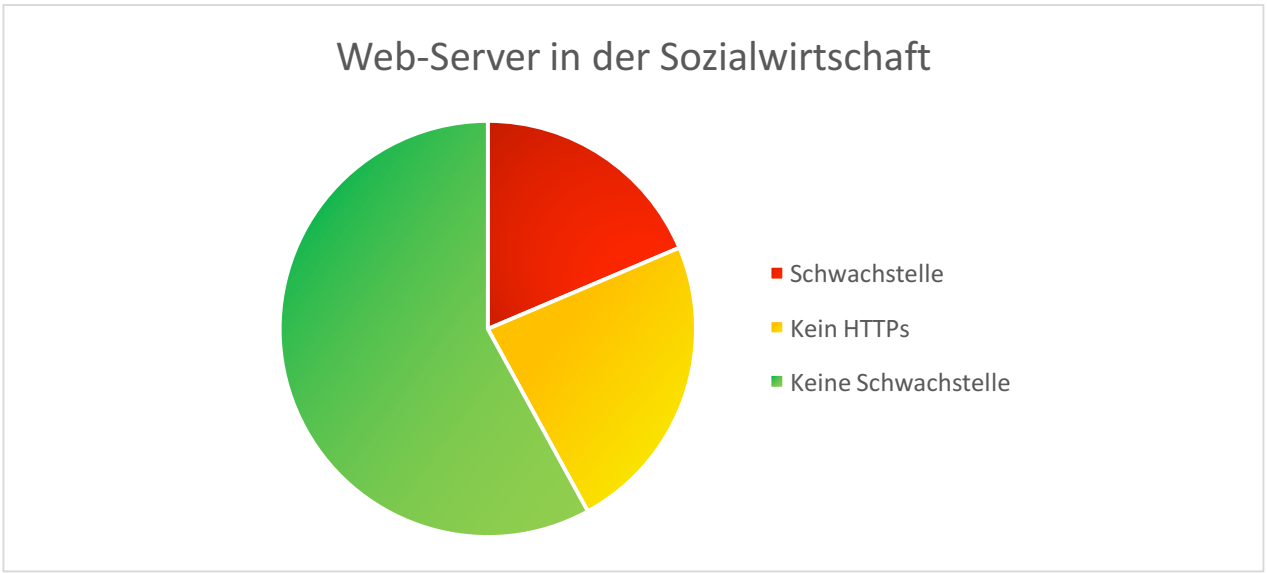

Abbildung 4: SSL-Schwachstellen bei 188 Web-Servern im Sozialwesen

Interpretation der Ergebnisse

Die Untersuchungsergebnisse zeigen: Ungefähr ein Viertel der untersuchten Organisationen erlauben keine verschlüsselten Verbindungen zu ihren Web-Servern. Von den Verbleibenden setzt ca. ein Viertel aller Organisationen veraltete Software mit Schwachstellen ein. Nur 58% der Organisationen scheinen ihre Web-Server-Software auf aktuellem Stand zu halten und Verschlüsselung für erforderlich zu halten.

Dies ist ein klares Indiz dafür, dass bei vielen Sozialunternehmen kein richtiges Sicherheitsmanagement existiert, welches die regelmäßige Aktualisierung und damit Schwachstellenbereinigung der Web-Server-Software vorsieht. Es lässt sich vermuten, dass dies auch für andere Organisations-IT gilt. Die Vorgaben des im Juli 2015 in Kraft getretenen IT-Sicherheitsgesetzes sind insofern vielfach nicht in der Praxis umgesetzt.

Aufgrund der Rahmenbedingungen wurde nur nach vier Schwachstellen gesucht. Es steht zu befürchten, dass eine weitaus umfangreichere Untersuchung einen deutlich höheren Anteil an verwundbaren Systemen aufdecken würde. Auch unterstützen nicht alle Unternehmen verschlüsselte Verbindungen, was aus Sicherheitsgründen der Fall sein sollte. Über diese Unternehmen liefert die Studie keine Zahlen bzgl. der Schwachstellen.

Handlungsempfehlung für Organisationen im Sozialwesen

Die untersuchten Sozialunternehmen sollten dringend ihr Sicherheitsmanagement überprüfen und gegebenenfalls anpassen. Regelmäßiges Einspielen von Sicherheitsupdates bzw. Software-Upgrades bei allen IT-Systemen stellt eine vergleichsweise einfache Sicherheitsmaßnahme mit großer Wirkung bzw. hohem Nutzen dar. Es kann auch sinnvoll sein, das Sicherheitsniveau von einem externen Dienstleister überprüfen zu lassen. Ebenso existieren Werkzeuge, wie z.B. *OpenVAS*, um die eigenen IT-Systeme auf Schwachstellen zu prüfen[1].

Konkret sich nur auf die hier beschriebenen Schwachstellen zu konzentrieren ist weder sinnvoll noch ausreichend. Ein Konzept zur regelmäßigen oder automatischen Durchführung von Softwareupdates einschließlich Überprüfung auf Umsetzung ist der einzige verlässliche Weg, um Schwachstellen möglichst schnell nach ihrer Veröffentlichung zu schließen.

[1] Die Autoren können bei Bedarf Auskunft zu der Studie bzw. den Schwachstellen geben und auch an einen Dienstleister zur Durchführung weitergehender Untersuchungen verweisen.

Zusammenfassung

Die Studie hat gezeigt, dass bei einer erheblichen Anzahl an Organisationen aus dem Sozialwesen Nachholbedarf bezüglich der Umsetzung IT-Sicherheitsmaßnahmen besteht. Der Einsatz von Verschlüsselung und regelmäßige Software-Updates im Rahmen des IT-Sicherheitsmanagements sind obligatorisch und verhindern, dass Schwachstellen, wie die hier untersuchten über das Internet ausgenutzt werden können.

Bei der Kommunikation mit Sozialunternehmen spielen Vertraulichkeit und Integrität eine besondere Rolle: Es kann jedem Betreiber von Websites nur empfohlen werden, https-geschützte Verbindungen anzubieten, diese regelmäßig auf Sicherheitslücken zu überprüfen und ein umfassendes IT-Sicherheitsmanagementsystem aufzubauen.