Studie zur Web-Server-Sicherheit von Unternehmen aus Hannover und Umgebung (2016)

Prof. Dr.-Ing. Peter Merz

Abstract

Der vorliegende Artikel beschreibt die Ergebnisse einer Studie zur Sicherheit von Web-Servern niedersächsischer Unternehmen aus dem Raum Hannover. Untersucht wurden vier Unternehmensgruppen die sich aus Mitgliedern von Unternehmensverbänden und berufsständischen Körperschaften zusammensetzen. Insgesamt werden mehr als 1800 Unternehmen betrachtet. Als Indikator für die IT-Sicherheit wurden vier Sicherheitslücken herangezogen, die leicht überprüft werden können ohne die Web-Server in ihrem Betrieb zu beeinträchtigen.

Die Ergebnisse sind ernüchternd: Viele Unternehmen setzen keine Verschlüsselung ein oder die Web-Server-Software ist nicht auf dem neusten Stand. Bei ungefähr jedem dritten Unternehmen, welches Verschlüsselung einsetzt, enthält die Software seit mehr als einem Jahr bekannte Schwachstellen und sollte umgehend aktualisiert werden. Dies zeigt, dass das IT-Sicherheitsmanagement in vielen Unternehmen mangelhaft ist.

Kontakt

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

Bedeutung der Web-Sicherheit für Unternehmen

Die Web-Präsenz eines Unternehmens ist Aushängeschild im Internet und längst für nahezu alle Unternehmen unverzichtbar. Deshalb sollte 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: Wird 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.

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 (Pentestern) gleichermaßen zur Verfügung.
Auch gibt es Suchmaschinen, wie *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-Server 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 im Tabelle 1 dargestellt sind.

Tabelle 1: SSL-Schwachstellen

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

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 Unternehmen

Insgesamt wurden vier Unternehmensgruppen untersucht. Die erste Gruppe (G1) besteht aus 1771 Unternehmen aus unterschiedlichen Branchen aus dem Raum Hannover (Unternehmen, die sich in der Online-Unternehmensdatenbank von HannoverImpuls[1] eingetragen haben). Die zweite Gruppe (G2) besteht aus 73 Unternehmen aus der IT-Branche ebenfalls aus dem Raum Hannover (Mitglieder Hannover-IT). In der dritten Gruppe (G3) befinden sich 549 Unternehmen aus dem Raum Niedersachsen (Mitglieder Unternehmerverband Niedersachsen - UVN). Die letzte Gruppe (G4) beinhaltet 96 der 100 größten Unternehmen gemessen an der Anzahl Beschäftigter aus der Region Hannover (Top 100 IHK Hannover). Die Gruppen sind nicht disjunkt; ein Unternehmen kann in mehreren Gruppen Mitglied sein.

Ergebnisse der Studie

Zunächst wurde mit Gruppe 1 die größte der vier Unternehmensgruppen durch Abfrage der Web-Server-Softwareversionen untersucht. Welche Web-Server-Implementationen eingesetzt werden, zeigt Abbildung 1.

[1] Zur Zeit der Artikelerstellung zu finden unter http://www.wirtschaftsfoerderung-hannover.de/hannoverimpuls/Unternehmensservice/Unternehmensdatenbank

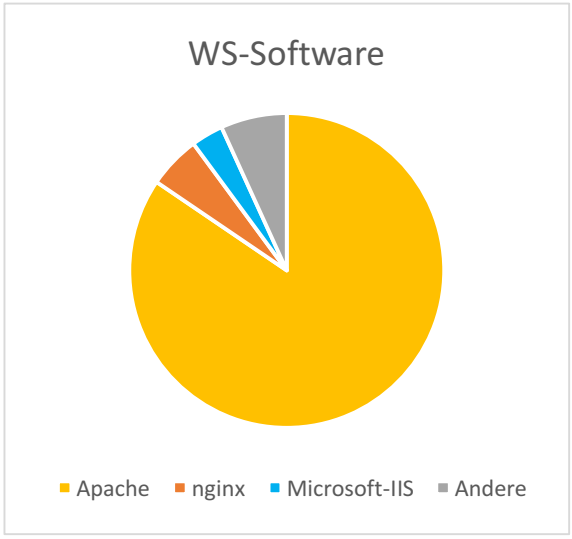

Abbildung 1: HTTP Server

Mit 84,5% ist Apache der am häufigsten eingesetzte Web-Server. Microsoft IIS hat nur einen Anteil von 3.3%. Welche Versionen von Apache eingesetzt werden, lässt sich nur zum Teil ermitteln, da 62.6% 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.

Die Betrachtung der eingesetzten PHP-Versionen liefert ein ähnliches Bild, wie in Abbildung 2 dargestellt.

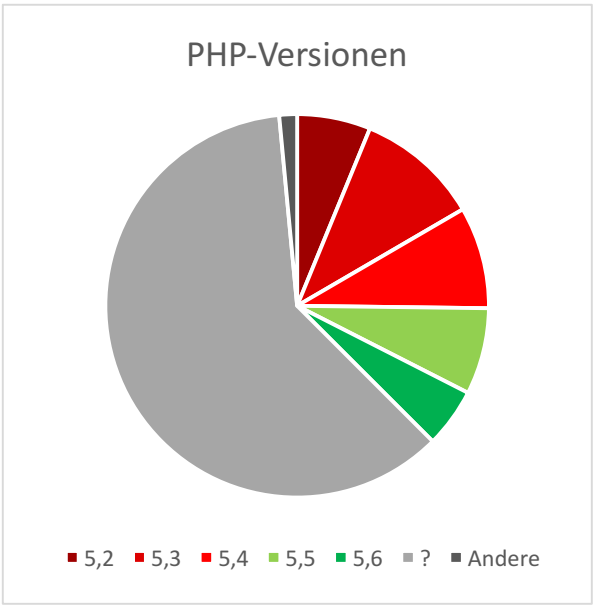

Abbildung 2: PHP-Versionen

Auch hier werden die Versionsnummern nur von einem Teil der Web-Server übertragen: 690 von 1771 HTTP-Servern geben diese Information preis. Von diesen 690 verwenden 58% Server PHP in einer Version kleiner als Version 5.5. Diese Zahl lässt einen großen Anteil an veralteter Softwareversionen mit möglichen Schwachstellen vermuten, da alle PHP-Versionen kleiner 5.5 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.

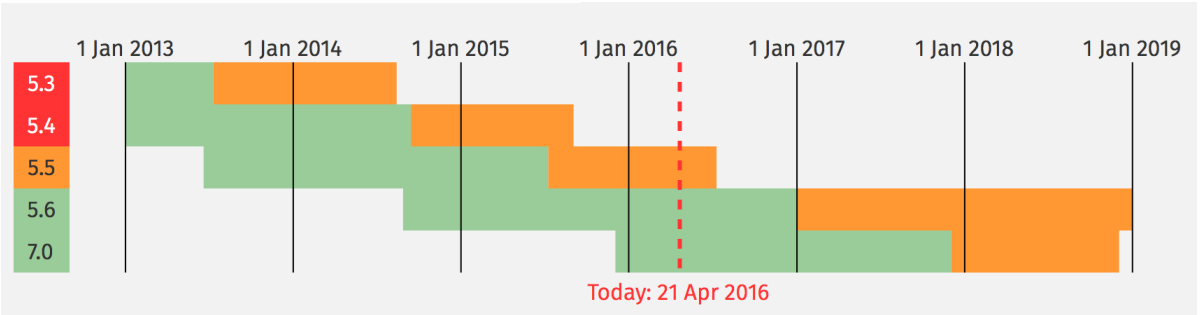

Abbildung 3: PHP-Lebenszyklen (Quelle: http://php.net/supported-versions.php)

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 1771 Unternehmen aus Gruppe G1 793 Web-Server keine verschlüsselten Verbindungen anbieten, wie in Abbildung 4 dargestellt.

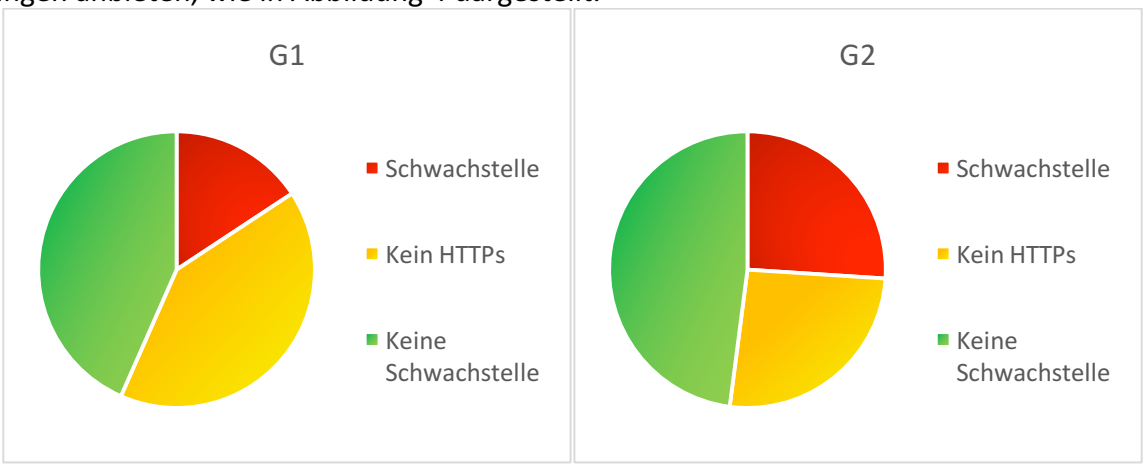

Abbildung 4: SSL-Schwachstellen bei Unternehmensgruppe G1 (HannoverImpuls) und G2 (Hannover-IT)

Von den verbleibenden Web-Servern enthalten 26,6% Schwachstellen.
Betrachtet man Unternehmen Gruppe G2 aus dem IT-Bereich, sind die Zahlen sogar alarmierender: 35,1% der HTTPS-Server, also diejenigen, die SSL-Verschlüsselung einsetzen, enthalten Schwachstellen. Immerhin ist hier der Prozentsatz der Server ohne Unterstützung für verschlüsselte Verbindungen geringer: 35,1% gegenüber 44,8%.
Bei Unternehmensgruppe G3 (Unternehmen aus Niedersachsen) zeigt sich, dass nur 27,1% der Web-Server keine Verschlüsselung anbieten, von den HTTPS-Servern aber 30,3% Schwachstellen in SSL aufweisen.

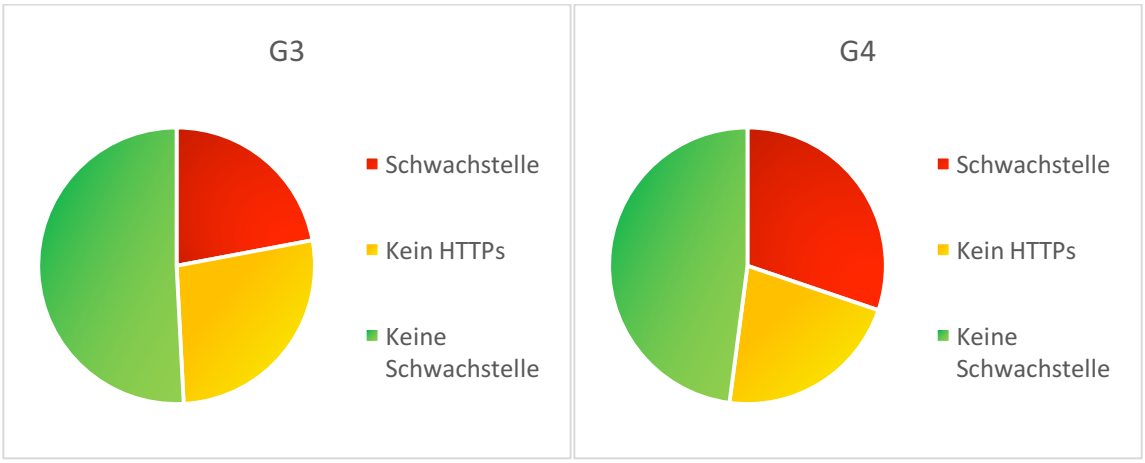

Abbildung 5: SSL-Schwachstellen bei Unternehmensgruppe G3 (UVN) und G4 (IHK-Top100)

Die letzte Gruppe G4 beinhaltet die Unternehmen mit der höchsten Anzahl Beschäftigter im Raum Hannover. Hier verwenden sogar 38,6% der HTTPS-Server Implementierungen von SSL mit Schwachstellen. Immerhin ist die Anzahl der Server ohne verschlüsselte Verbindungen mit 21 von 96 (21,9%) geringer als bei den anderen Unternehmensgruppen.

Interpretation der Ergebnisse

Die Untersuchungsergebnisse zeigen: ca. ein Drittel aller Unternehmen setzt veraltete Software mit Schwachstellen ein. Dies ist ein klares Indiz dafür, dass bei vielen Unternehmen 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 Unternehmens-IT gilt. Aufgrund der Rahmenbedingungen wurde nur nach vier Schwachstellen gesucht. Eine weitaus umfangreichere Untersuchung hätte wohlmöglich einen noch höheren Anteil an verwundbaren Systemen gefunden. 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. Überraschend ist auch, dass auch die größten Unternehmen (bzgl. Beschäftigtenzahl) im Raum Hannover nicht besser als die kleineren dastehen. Im Gegenteil: Hier ist der Anteil der anfälligen Server mit 38,6% am höchsten. Vergleicht man die Unternehmensgruppen G1 und G2, fällt auf, dass es in der Gruppe der IT-Unternehmen (G2) mit der Sicherheit schlechter bestellt ist. Eine mögliche Erklärung ist, dass IT-Unternehmen ihrer Web-Server häufig selbst betreiben, da sie das Know-How dazu haben, sich aber nicht konsequent um die Sicherheit dieser kümmern. Ein Grund, warum die Gruppe G1 im Vergleich mit allen anderen Gruppen am besten abschneidet, ist wohlmöglich, dass in dieser Gruppe eine hohe Anzahl an Web-Hostern für das Betreiben der Web-Server zuständig ist, und diese ein ausreichendes Sicherheitsmanagement implementieren.

Handlungsempfehlung für Unternehmen

Die Unternehmen im Raum Hannover 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[2].
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.

Zusammenfassung

Die Studie hat gezeigt, dass bei einer erheblichen Anzahl an Unternehmen im Raum Hannover bzw. Niedersachsen ein Nachholbedarf bezüglich IT-Sicherheit besteht. Der Einsatz von Verschlüsselung und regelmäßige Softwareupdates im Rahmen des IT-Sicherheitsmanagements sind obligatorisch und verhindern, dass Schwachstellen, wie die hier untersuchten über das Internet ausgenutzt werden können.

[2] Der Autor kann bei Bedarf Auskunft zu der Studie bzw. den Schwachstellen geben und auch an einen externen Dienstleister verweisen.