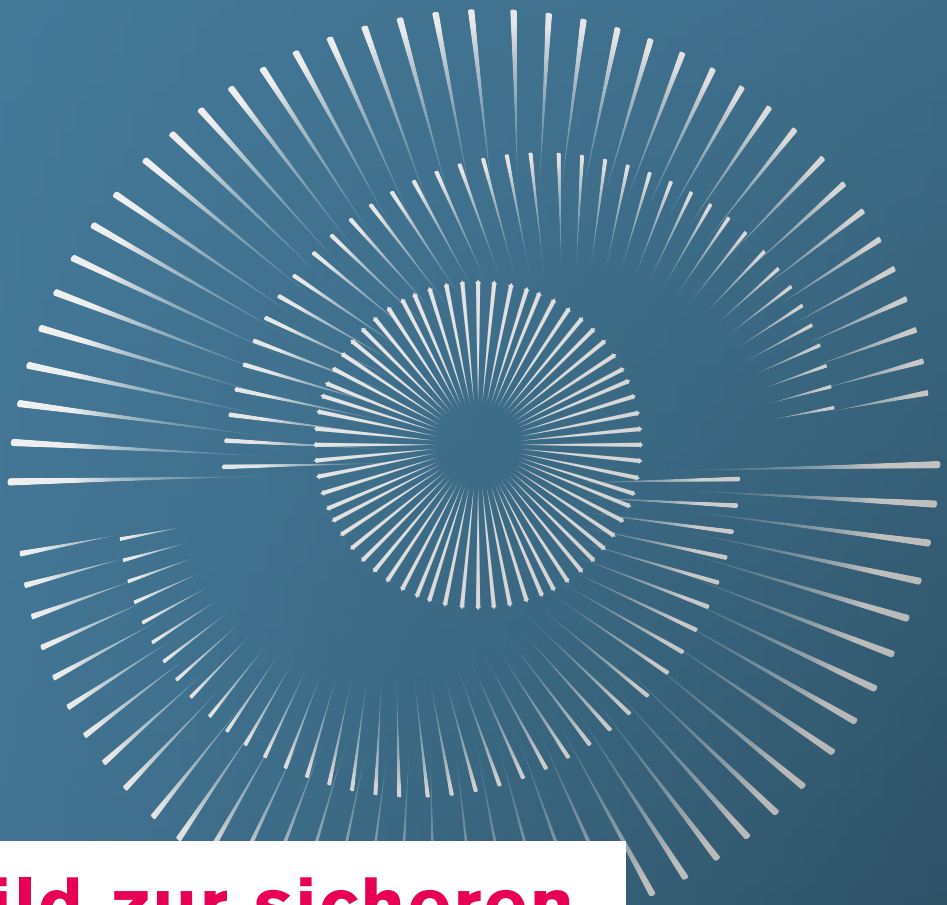
HSA_innos
Institut für innovative Sicherheit

Technologie-transferzentrum Data Analytics

Hochschule Augsburg University of Applied Sciences



Lagebild zur sicheren Kommunikation mit Webseiten aus dem Landkreis Donau-Ries 2021

Eine Studie des Instituts für innovative Sicherheit (HSA_innos) und des Technologietransferzentrums (TTZ) Data Analytics der Hochschule Augsburg

HSA_innos
Institut für innovative
Sicherheit

Technologie-
transferzentrum
Data Analytics

Hochschule
Augsburg University of
Applied Sciences

Die beiden Forschungsinstitute HSA_innos
und TTZ arbeiten für den Transfer
von wissenschaftlichen Erkenntnissen
in die gesellschaftliche und wirtschaftliche Praxis.
Sie sind Teil der Hochschule Augsburg.
Die folgende Studie ist in enger Zusammen-
arbeit beider Institute entstanden.

Autoren: Fabian Bley, Florian Ernst, Benjamin Kienle
Betreuer: Prof. Dr. Dominik Merli

Über das Institut für innovative Sicherheit (HSA_innos)

HSA_innos hilft Unternehmen dabei, sich individuell zu schützen. Neben der Aus- und Weiterbildung von Sicherheitsexperten liegt der Schwerpunkt des Instituts auf der Entwicklung von Technologien und Prozessen für die IT-Sicherheit zur Anwendung in der Praxis. Zusammen mit HSA_innos schützen Unternehmen und andere Organisationen ihre Investitionen und Kunden vor digitalen Bedrohungen.

www.hsainnos.de

HSA_innos
Institut für innovative Sicherheit

Über das Technologie-transferzentrum (TTZ) Data Analytics in Donauwörth

Das TTZ Data Analytics macht das Potenzial von Daten und Digitalisierung für Unternehmen nutzbar. Forschung und Industrie entwickeln gemeinsam datenbasierte Lösungen und Konzepte zur sicheren und digitalen Wertschöpfung.
Der Landkreis Donau-Ries soll so die Möglichkeit bekommen, sich auf die digitalisierte Zukunft vorzubereiten.

www.ttz-data-analytics.de

Technologie-
transferzentrum
Data Analytics

Inhaltsverzeichnis

Vorwort

Unternehmen, Behörden und Vereine nutzen alle eigene Internetseiten, um Kund:innen, Bürger:innen und Mitglieder schnell mit Informationen zu versorgen. Allerdings dienen diese Webpräsenzen nicht mehr nur der reinen Information. Sie werden vermehrt auch zum Austausch vertraulicher und personenbezogener Daten eingesetzt. Deshalb spielen Datensicherheit und Datenschutz für die Kommunikationsverbindung zwischen den Nutzenden und der Webseite eine wichtige Rolle. Denn so können Betreiber möglichen Angriffen entgegenwirken und Vertrauen in die bereitgestellte Plattform aufbauen.

In der vorliegenden Studie wird das Lagebild zur sicheren Kommunikation mit Internetseiten von Unternehmen und Organisationen untersucht, die im Landkreis Donau-Ries ansässig sind. Hierzu wurden 3437 Domains identifiziert und untersucht.

Ziel war es, die Umsetzung des Stands der Technik zu analysieren und ein Bewusstsein für die involvierten Sicherheitsrisiken zu schaffen. Zudem dient diese Arbeit als Basis für die Entwicklung gezielter, regionaler Unterstützungsangebote für Firmen und Organisationen.

Ausgangslage

Ein ansprechender Internetauftritt ist ein wichtiger Faktor bei der Kommunikation von Organisationen aller Größen. Unternehmen, Behörden, Handwerksbetriebe, Arztpraxen oder regionale Vereine – stets müssen Informationen für Kund:innen, Bürger:innen und Mitglieder bereitstehen. Denn eine Webseite dient oft als erste Anlaufstelle für Interessierte und trägt damit wesentlich zur Außenwirkung bei.

Allerdings ist reine Kommunikation nicht mehr die einzige Funktion von Webseiten. Zunehmend werden dort auch individuelle Daten heruntergeladen oder Dateien und Informationen der Nutzenden an die Webanwendung übermittelt. Dabei kann es sich auch um personenbezogene Daten sowie sensible Finanz-, Sicherheits- oder Gesundheitsdaten handeln. Gerade dann ist es unabdingbar, die Vertraulichkeit und Integrität der ausgetauschten Daten zu gewährleisten. Andernfalls besteht die Gefahr, dass Daten manipuliert, Informationen gestohlen oder Online-Aktivitäten ausspioniert werden.

Sicherheitsvorkehrungen von Webseiten sind oftmals unzureichend

Obwohl bei Internetanwendungen hohe Sicherheitsanforderungen notwendig sind [5], schützen Betreiber ihre Internetseiten oftmals nur unzureichend. Dies zeigen zahlreiche Studien, unter anderem eine des Fachverbands deutscher Webseiten-Betreiber aus dem Jahr 2020 [1]. Darin wurden 2500 zufällig ausgewählte Webauftritte kleiner und mittlerer Unternehmen bezüglich ihrer Sicherheit beurteilt.

Neben anderen Kriterien untersuchte die Studie des Fachverbands, ob ein aktives und funktionierendes digitales Zertifikat zur Authentifizierung einer Webadresse [4] verwendet wird.[1] Das Ergebnis: 36 Prozent der untersuchten Webseiten verwendeten kein gültiges, funktionierendes Zertifikat und stellten somit ein Risiko für die jeweiligen Nutzer:innen dar. Darüber hinaus wiesen insgesamt 41 Prozent der untersuchten Internetseiten nachweisbare Sicherheitsmängel auf.

Eine weitere Analyse kleiner und mittelständischer Unternehmen im Rahmen des Projekts „Sichere Webseiten und Content Management Systeme“ (SIWECOS) fand zudem heraus, dass im November 2019 etwa jede zweite Firmenwebseite potenziell angreifbar war [10]. Derartige Ergebnisse zeigen, dass trotz der fortschreitenden Digitalisierung ein erheblicher Anteil an Webpräsenzen nicht nach dem aktuellen Stand der Technik abgesichert ist. Nutzer:innen können damit nicht immer auf eine sichere Kommunikationsverbindung vertrauen.

Wie ist die Lage im Donau-Ries?

Die vorliegende Studie zeichnet ein spezifisches, regionales Bild zur Lage der sicheren Kommunikation von Webseiten, die in Verbindung mit Organisationen aus dem Landkreis Donau-Ries stehen. Zudem werden Fehlkonfigurationen identifiziert und ein Bewusstsein für Risiken geschaffen. Letztendlich soll dies die IT-Sicherheit von Internetseiten lokaler Institutionen erhöhen und das Vertrauen der Nutzer:innen in diese Technologie stärken.

1 Ein digitales Zertifikat ermöglicht es einem Webserver seine Echtheit / Identität nachzuweisen.

Grundlagen sicherer Kommunikation im Internet

Webpräsenzen sind nicht automatisch sicher. Sie müssen richtig konfiguriert werden. So schaffen Betreiber:innen ein sicheres und vertrauenswürdiges Online-Erlebnis.

Wichtig ist zu verstehen, wie die Kommunikation zwischen Webseiten und Nutzer:innen funktioniert. Diese erfolgt nach dem sogenannten Client-Server-Modell. Hierbei agiert das System der Nutzer:innen, üblicherweise ein Internetbrowser, als Client. Der Server ist das System, auf dem der Webauftritt betrieben wird. Beim Aufrufen einer Internetseite, dem Abschicken eines Formulars oder dem Download eines Dokuments werden Daten zwischen Client und Server ausgetauscht. Die Sicherheit dieser Verbindung hängt sowohl von den verwendeten Technologien als auch deren Konfiguration ab. Beides wird in den folgenden Abschnitten erläutert.

HTTP garantiert keine sichere Verbindung

Die Verbindung zwischen Client und Server kann von Dritten ausgespäht und manipuliert werden, wenn die Datenübertragung über das ungesicherte Hypertext Transfer Protocol (HTTP) stattfindet.[2] Zudem können Nutzer:innen sich bei Verwendung von HTTP nicht sicher sein, dass sie tatsächlich mit der echten Webseite verbunden sind oder ob der Kommunikationskanal von Angreifern kompromittiert wurde. Dies stellt ein beträchtliches Risiko für Nutzer:innen und deren Daten dar. Anders das Protokoll HTTPS.

Nur HTTPS in korrekter Konfiguration ist sicher

Das Hypertext Transfer Protocol Secure (HTTPS) gewährleistet eine sichere Kommunikation, denn es ermöglicht eine verschlüsselte sowie gegen Manipulationen geschützte Datenübertragung [7]. Für den Laien lässt sich dies an der Webadresse im Browser feststellen, der ein „https“ vorangestellt sein sollte.

Die Sicherheit von HTTPS baut wiederum auf das Protokoll Transport Layer Security (TLS) auf, das in früheren Versionen Secure Socket Layer (SSL) genannt wurde. Doch auch TLS ist nicht automatisch sicher. Hier gilt es einiges zu beachten.

Sicher im Netz mit kryptographischen Verfahren

Auch TLS bietet nur dann die gewünschte Sicherheit, wenn aktuelle kryptographische Verfahren [3] zur Verschlüsselung eingesetzt werden und die Konfiguration des Webservers dem Stand der Technik entspricht. Kommen veraltete Protokollversionen zum Einsatz oder wurden kryptographische Parameter zu schwach gewählt, besteht weiterhin ein Sicherheitsrisiko für die Daten der Nutzer:innen.

Konkret gelten mittlerweile alle Versionen von SSL sowie die TLS-Versionen 1.0 und 1.1 als veraltet [3, 9]. Als sicher werden demnach lediglich die Protokolle TLS 1.2 und TLS 1.3 angesehen, die auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt [3]. Zudem sollten beim Einsatz von TLS 1.2 die angebotenen kryptographischen Algorithmen zur Verschlüsselung (sogenannte Cipher Suites) auf moderne und sichere Varianten beschränkt werden. Hierbei wird empfohlen, nur auf Cipher Suites zurückzugreifen, die die sogenannte Perfect Forward Secrecy (PFS)[3] unterstützen [3].

Zertifikate müssen vertrauenswürdig sein

Außerdem muss die Authentifizierung des Webservers auf Basis eines aktuellen, vertrauenswürdigen X.509-Zertifikats passieren [4]. Diese digitalen Zertifikate werden von sogenannten Certificate Authorities (CA) ausgestellt, die die Korrektheit der Zertifikatsdaten gewährleisten. Des Weiteren sollten bei X.509-Zertifikaten die aktuell vom BSI empfohlenen Schlüssellängen beachtet werden. Für RSA-basierte[4] Zertifikate sollte eine Schlüssellänge von mindestens 2000 Bit zum Einsatz kommen. RSA kommt bei den meisten Zertifikaten zum Einsatz. Moderner sind Verfahren auf Basis elliptischer Kurven (Elliptic Curve Digital Signature Algorithm, kurz: ECDSA). Hier sollten Schlüssel mit einer Länge von mindestens 250 Bit eingesetzt werden [3, 6]. Aufgrund der geringeren Länge der Schlüssel bei gleicher Sicherheit, können Signaturen auf Basis von ECDSA schneller generiert werden als beim RSA-Verfahren.

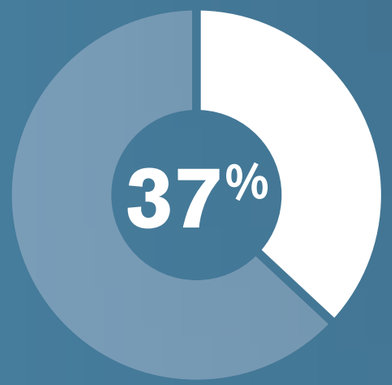
2 Protokolle definieren den Ablauf einer Kommunikation und das verwendete Nachrichtenformat.

3 Perfect Forward Secrecy ist eine Eigenschaft von kryptographischen Protokollen für den Schlüsselaustausch. Sie besagt, dass kurzlebige Sitzungsschlüssel so ausgetauscht werden, dass sie selbst dann nicht rekonstruiert werden können, wenn Dritte in der Zukunft Zugriff auf die verwendeten Langzeitschlüssel haben.

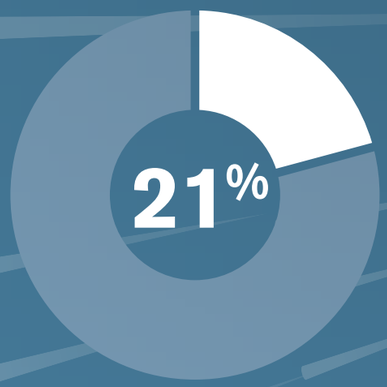
4 RSA ist ein Akronym der Nachnamen der Erfinder des Verfahrens: Rivest, Shamir, Adleman.

Zusammenfassung der wichtigsten Erkenntnisse

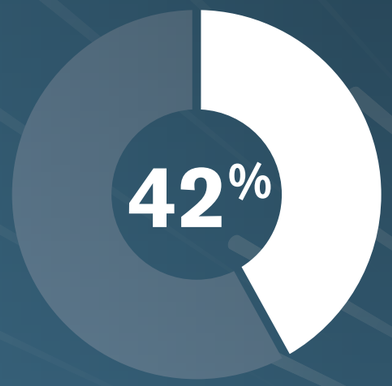
Wie sicher ist die Kommunikation mit Webseiten im Donau-Ries? Fünf Kernaussagen unserer Studie beleuchten diese Frage und zeigen deutlich: Oft besteht Nachholbedarf.



Lediglich 37 Prozent der untersuchten Webseiten genügen aktuellen Empfehlungen und bieten ihren Nutzer:innen damit sichere Kommunikation.

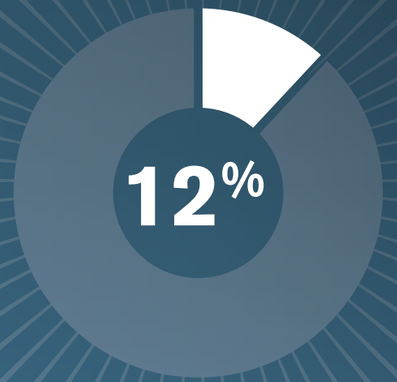


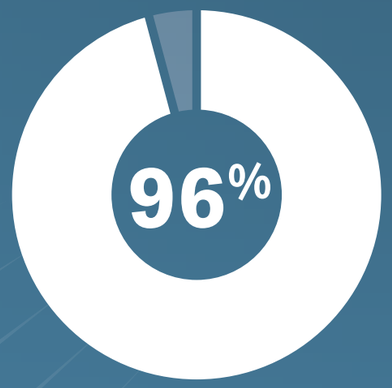
Bei 21 Prozent der analysierten Internetauftritte wurden geringfügige Konfigurationsfehler identifiziert. Damit haben sie ein annehmbares Sicherheitsniveau. Dennoch sind auch bei diesen Seiten gezielte Nachbesserungen nötig, um eine noch vertrauenswürdigere Kommunikationsverbindung zu schaffen.



Bei 42 Prozent der untersuchten Webauftritte konnten erhebliche Mängel bei der Verbindungssicherheit festgestellt werden.

12 Prozent der überprüften Webseiten nutzten lediglich HTTP und boten damit keine Form einer sicheren Kommunikation an. Die Mehrheit dieser Seiten gehört regionalen Unternehmen.



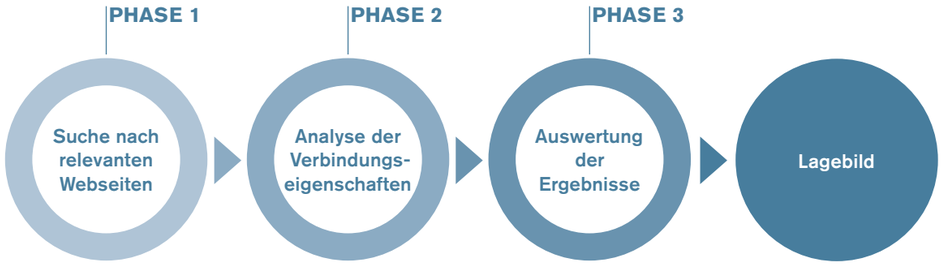


96 Prozent der untersuchten HTTPS-Webseiten nutzen gültige digitale Zertifikate, die die Authentizität des verwendeten Webservers garantieren.

Vorgehensweise

Unsere Methodik führt zu einem konkreten regionalen Lagebild der Kommunikationssicherheit.

Die Untersuchung gliederte sich in drei Phasen (siehe Grafik). Wir identifizierten zuerst Internetseiten mit Bezug zum Landkreis Donau-Ries und sammelten sie in einer Datenbank. Anschließend wurden diese Webseiten mit unterschiedlichen Sicherheitsparametern angefragt und die jeweiligen Antworten analysiert. Die abschließende Auswertung der ermittelten Daten zeichnet ein regionales Lagebild zur sicheren Kommunikation mit Webpräsenzen.



Grafik: Überblick über die einzelnen Phasen dieser Studie

Phase 1:
Suche nach relevanten Webseiten

Der erste Schritt der Analyse bestand darin, die Webseiten auf einen spezifischen Landkreis einzugrenzen. Eine Lokalisierung auf Basis von IP-Adressen führte nicht zum Ziel. Denn die Webseiten werden nicht zwingend auf Servern im Landkreis Donau-Ries betrieben, sondern können weltweit bei verschiedensten Anbietern platziert sein. Deshalb führten wir für die vorliegende Studie eine automatische Suche mittels geeigneter Google-Anfragen durch, die Postleitzahlen, Ortsnamen und Branchenbezeichnungen verknüpfte. Anschließend wurden die daraus resultierenden Suchergebnisse anhand des Impressums und der angegebenen Kontaktdaten automatisiert sowie in Einzelfällen manuell validiert. Die so generierte Datenbank diente als Grundlage für die nachfolgenden Phasen der Studie.

Phase 2:
Analyse der Verbindungs-eigenschaften

Zur Analyse der Webserver-Konfigurationen sowie der Verbindungssicherheit der jeweiligen Internetseiten nutzten wir das Software-Werkzeug SSLyze [2]. Dieses Tool ermöglicht unter anderem die Ermittlung der unterstützten SSL- und TLS-Versionen sowie die Auswertung der bereitgestellten digitalen Zertifikate.

Zudem wurde im Rahmen dieser Studie eine Software entwickelt, die die ermittelten Rohinformationen von SSLyze automatisiert in eine einheitliche, analysierbare Struktur konvertierte. Zu den darin gesammelten Kriterien der Untersuchung zählten unter anderem die Verwendung von HTTPS, der Einsatz von geeigneten TLS-Protokollversionen und ob X.509-Zertifikate mit einer entsprechenden Gültigkeit eingesetzt wurden.

Phase 3:
Auswertung der Ergebnisse

Im Anschluss an die automatisierte Analyse wurden die Ergebnisse inhaltlich ausgewertet. Dies gab Aufschluss, ob und in welchem Umfang die untersuchten Server sicher konfiguriert sind und ob sie den Nutzer:innen damit ausreichenden Schutz bieten. Im Umkehrschluss wird somit erkennbar, wie groß der Anteil der Webseiten aus dem Landkreis Donau-Ries ist, die zum Zeitpunkt der Studie veraltete bzw. unsichere Konfigurationen verwendeten und somit ein Sicherheitsrisiko für Nutzer:innen darstellten.

Die Ergebnisse wurden abschließend dazu verwendet, um Betreiber von unzureichend geschützten Internetseiten zu kontaktieren und auf die Sicherheitsrisiken aufmerksam zu machen. Zusätzlich gaben wir den Betroffenen Hinweise, was geeignete Maßnahmen für ein angemessenes Sicherheitsniveau wären. Dadurch soll sich das Sicherheitsniveau der Internetseiten im Landkreis Donau-Ries erhöhen.

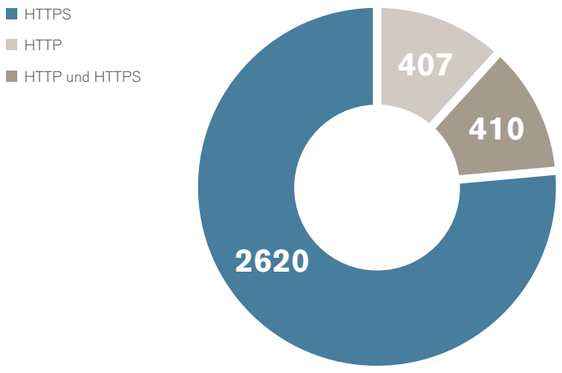
Ergebnisse der Untersuchung im Detail

Mehrheit der untersuchten Seiten nutzt HTTPS-Verbindungen

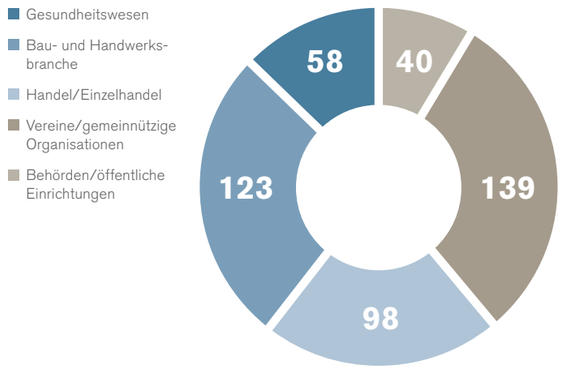
Im August 2021 ergab die automatisierte Identifikation relevanter Internetseiten für den Landkreis Donau-Ries insgesamt 3437 Domains. Davon ermöglichten 3030 Seiten eine Verbindung mittels HTTPS. Keine korrekte Umleitung von HTTP auf HTTPS implementierten 410 Webauftritte und stellten somit beide Kommunikationskanäle zur Verfügung (siehe Grafik 1). Bezüglich der HTTPS-Verbindungen erlaubten 3025 Seiten eine automatisierte Analyse mittels SSLyze. Lediglich fünf Webseiten konnten nicht untersucht werden. Die verbleibenden 407 Webpräsenzen (12 Prozent aller identifizierten Domains) nutzten lediglich HTTP und boten damit keine Form einer sicheren Kommunikation an.

Großteil der unsicheren HTTP-Verbindungen stammt von regionalen Unternehmen

Beim Großteil aller Webseiten, die über einen HTTP-Kanal erreichbar waren, handelte es sich um Webseiten kleiner und mittelgroßer Unternehmen. Die Branchen sind wie folgt aufgeteilt: 58 Seiten stammen aus dem Gesundheitswesen, 123 aus der Bau- und Handwerksbranche und 98 aus dem Handel oder Einzelhandel. Außerdem waren 139 Internetauftritte von Vereinen und gemeinnützigen Organisationen und 40 weitere von Behörden und öffentlichen Einrichtungen nur durch HTTP erreichbar (siehe Grafik 2).



1 Grafik: Gegenüberstellung von HTTP- und HTTPS-Verbindungen



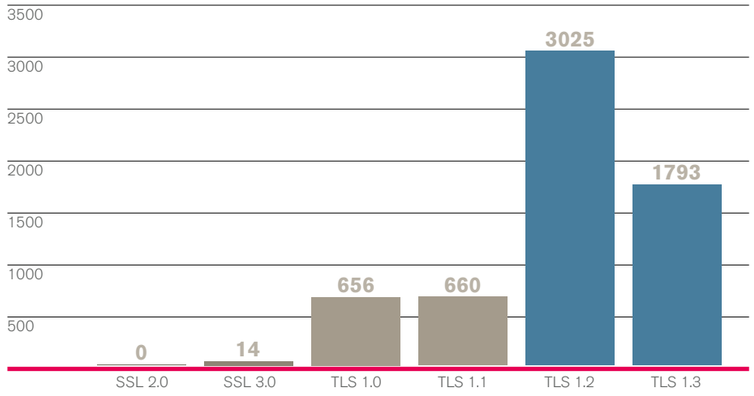
2 Grafik: Branchenverteilung der untersuchten HTTP-Webseiten

Veraltete Protokolle erlauben Downgrade-Angriffe

Die Protokollanalyse zeigt, dass bei allen überprüften HTTPS-Verbindungen die Version TLS 1.2 angeboten wurde. Außerdem ermöglichten 59 Prozent die Verwendung der aktuellsten Version TLS 1.3. Dennoch ließen sich Probleme bei der konkreten Konfiguration erkennen. Denn es wurden weiterhin veraltete und unsichere Kommunikationsprotokolle wie TLS 1.0, TLS 1.1 oder gar SSL 3.0 erlaubt (siehe Grafik 3).

Jedoch konnte keine Seite identifiziert werden, die ausschließlich über unsichere SSL- oder TLS-Varianten kommunizierte. 22 Prozent der untersuchten Seiten, die ausschließlich HTTPS nutzten, stellten sowohl sichere als auch veraltete Algorithmen für die Kommunikation bereit. Demgegenüber standen 78 Prozent, die ausschließlich die empfohlenen kryptographischen Protokolle TLS 1.2 und TLS 1.3 anboten.

Das Anbieten veralteter Protokolle ist vor allem deswegen riskant, da Angreifende dies durch sogenannte Downgrade-Angriffe [8] ausnutzen können. Deshalb sollten nicht nur die empfohlenen kryptographischen Algorithmen angeboten, sondern auch alle unsicheren Protokolle nicht mehr zur Verfügung gestellt werden.



3 Grafik: Verteilung der Protokollversionen

Sichere Konfiguration von TLS 1.2

Bei Webseiten, die das Protokoll TLS 1.2 nutzten, untersuchten wir die eingesetzten Cipher Suites. 52 Prozent der analysierten Internetseiten unterstützten ausschließlich Cipher Suites mit PFS (siehe Grafik 4). Alle verbleibenden Webseiten, die TLS 1.2 bereitstellten, verwendeten zusätzlich mindestens eine Cipher Suite, die keine PFS ermöglichte.

Mehrheit verwendet sichere Zertifikate

Neben verschlüsselten Datenverbindungen wurden auch die X.509-Zertifikate analysiert, die die Authentizität des jeweiligen Webservers sicherstellen. Hier besaßen 96 Prozent der Internetseiten, die eine HTTPS-Verbindung anboten, gültige Zertifikate. 4 Prozent der untersuchten Zertifikate wurden als ungültig und damit unsicher eingestuft.

Die Grafik 5 zeigt die Verteilung der unterschiedlichen Gründe für die Ungültigkeit bestimmter Zertifikate. Insgesamt wurden 64 selbstsignierte[5] Zertifikate, 31 mit abgelaufenem Gültigkeitszeitraum und 28 mit einer unvollständigen Zertifikatskette[6] ermittelt. Zusätzlich überschritten 58 Zertifikate den maximal zulässigen Gültigkeitszeitraum. Dabei ist anzumerken, dass die maximale Zertifikatslaufzeit von großen Browseranbietern wie Apple, Google und Mozilla seit Oktober 2020 auf 398 Tage beschränkt wurde [11, 12, 13]. Demzufolge werden alle Zertifikate, die länger als 398 Tage gültig sind, von den jeweiligen Browsern als unsicher eingestuft. Die dargestellten Ergebnisse zeigen, dass bei der Mehrheit der untersuchten Webseiten gültige digitale Zertifikate eingesetzt werden.

Let's Encrypt ist die beliebteste Certificate Authority

Die analysierten Zertifikate lassen sich nach Certificate Authorities eingruppieren (siehe Grafik 6). 45 Prozent aller untersuchten X.509-Zertifikate stellte Let's Encrypt aus. Dies ist eine Non-Profit-Organisation, die seit 2015 kostenlose digitale Zertifikate ausstellt [14] und die Kommunikationssicherheit mittels HTTPS erhöhen möchte. Danach folgten unter anderem die kommerziellen Anbieter DigiCert mit 34 Prozent und Sectigo mit 8 Prozent. Damit geht die Tendenz eindeutig zum Non-Profit Anbieter.

Die Mehrheit der untersuchten Webauftritte nutzte digitale Zertifikate mit kryptographischen Schlüsseln von angemessener Länge. Bei allen Seiten, die das ECDSA-Verfahren verwendeten, war die gewählte Schlüssellänge größer als 250 Bit. Bei lediglich 2 Prozent der untersuchten RSA-Schlüssel war die Länge zu kurz, um den aktuellen Empfehlungen des BSI zu entsprechen. Zudem boten nur 20 von 3025 HTTPS-Seiten ein X.509-Zertifikat auf Basis des ECDSA-Verfahrens an. 3005 Webseiten verwendeten RSA-basierte Zertifikate.

Mehr als 40 Prozent der untersuchten Webseiten wiesen erhebliche Fehler auf

Abschließend wurden die analysierten Webauftritte in drei Gruppen eingeordnet (siehe Grafik 7).

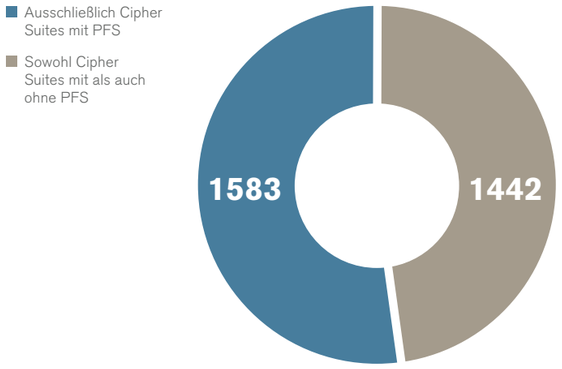
- Konfiguration gemäß dem Stand der Technik: Domains, die HTTPS nur mittels TLS 1.2 inklusive PFS sowie TLS 1.3 anboten und ein gültiges X.509-Zertifikat besaßen. Diese Verbindungen entsprechen den aktuellen Empfehlungen.
- Geringfügige Konfigurationsfehler: Domains, die Cipher Suites ohne PFS und zu kurze Schlüssellängen bei ECDSA bzw. RSA einsetzten. Diese Verbindungen sind nicht auf dem neuesten Stand und könnten optimiert werden.
- Erhebliche Konfigurationsfehler: Domains, die eine HTTP-Verbindung anboten, die bei HTTPS veraltete Protokollversionen ermöglichten und die Zertifikatsfehler aufwiesen. Diese Verbindungen sind unsicher.

1264 Seiten waren bezüglich der Kommunikationssicherheit auf dem neuesten Stand. 732 wiesen geringfügige Mängel bei der Konfiguration auf. Insgesamt wurden 1436 Internetseiten mit erheblichen Sicherheitsmängeln identifiziert.

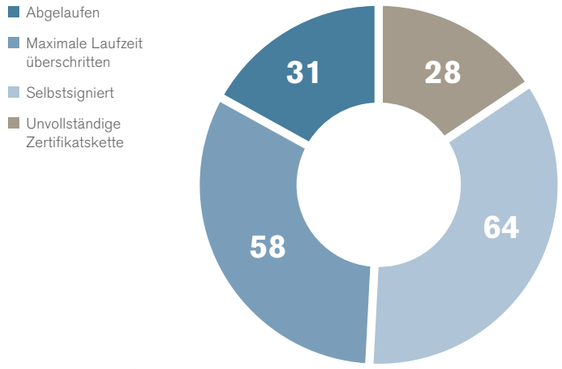
Darüber hinaus verweisen wir auf besonders bedenkliche Fälle, die wir im Rahmen der Studie identifiziert haben. Beispielsweise wurden zwei X.509-Zertifikate gefunden, die eine Laufzeit bis ins Jahr 2115 aufwiesen. Dies übersteigt deutlich den Richtwert von 398 Tagen. Zudem wurden 60 Seiten ermittelt, die die Kommunikationsverbindung vom sicheren HTTPS-Protokoll auf die unsichere HTTP-Variante umleiteten. Dies zeigt, dass der Kommunikationssicherheit von Webseiten teilweise keinerlei Beachtung geschenkt wird.

5 Selbstsignierte Zertifikate wurden nicht durch eine vertrauensvolle Certificate Authority ausgestellt.

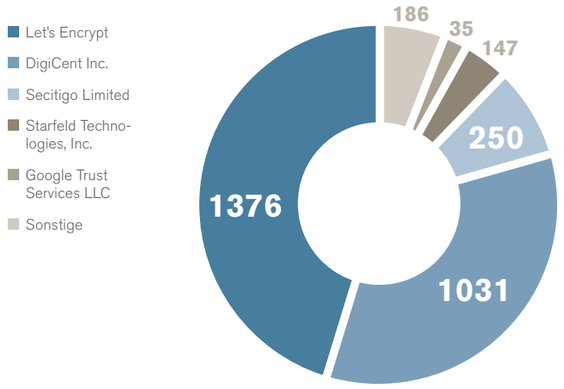
6 Eine Zertifikatskette ist eine Liste von Zertifikaten, die für die Authentifizierung eines Webservers notwendig ist. Dieser Zertifizierungspfad bildet eine Vertrauenskette bis zur Stammzertifizierungsstelle.



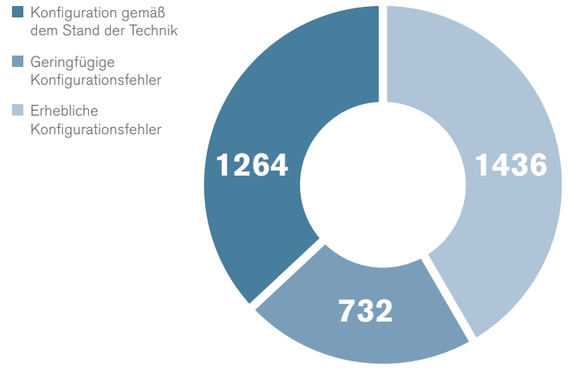
4 Grafik: Verwendete Cipher Suites bei TLS 1.2 Verbindungen



5 Grafik: Gründe für die Ungültigkeit der untersuchten X.509-Zertifikate



6 Grafik: Anzahl ausgestellter X.509-Zertifikate je Certificate Authority



7 Grafik: Kategorisierung der untersuchten Webpräsenzen

Fazit

Bei 63 Prozent der Webseiten im Donau-Ries können gezielte Maßnahmen die Kommunikationssicherheit deutlich verbessern. Darunter: Unternehmen, Behörden und Vereine.

Die vorliegende Studie untersuchte insgesamt 3432 Internetauftritte aus dem Landkreis Donau-Ries hinsichtlich ihrer Kommunikationssicherheit. Die Ergebnisse zeigen, dass lediglich 37 Prozent der analysierten Webseiten vollständig dem aktuellen Stand der Technik entsprachen, sichere Kommunikationsprotokolle anboten sowie gültige digitale Zertifikate verwendeten.

Bei allen anderen Webseiten konnten wir Verbesserungspotenzial identifizieren. Hier sind insbesondere die 407 Seiten zu nennen, die bisher nur unsichere HTTP-Verbindungen anboten und hauptsächlich Unternehmen, aber auch Behörden und Vereinen zuzuordnen sind. Bei 1761 Webauftritten mit aktivierter HTTPS-Verbindung wurden Fehlkonfigurationen erkannt, die durch gezielte Verbesserungen behoben werden können. Eine Umsetzung dieser Maßnahmen erhöht die Verbindungssicherheit dieser Seiten und ermöglicht den Nutzer:innen eine vertrauenswürdige Kommunikation im Internet.

In diesem Zusammenhang sollte vor allem im Bereich der angebotenen TLS-Versionen nachgebessert werden, sodass die betroffenen Seiten ausschließlich sichere Protokollversionen und moderne Cipher Suites verwenden. Außerdem sollte sich jede Webpräsenz über ein gültiges X.509-Zertifikat einer vertrauenswürdigen Certificate Authority ausweisen können.

Wir haben mit 807 Betreiber:innen von Webseiten, die unsichere HTTP-Verbindungen verwenden und Zertifikatsfehler aufwiesen, Kontakt aufgenommen. Hierbei haben wir sie über die Mängel informiert und Handlungsempfehlungen gegeben.

Zusammenfassend lässt sich feststellen, dass die Mehrheit der untersuchten Seiten die Voraussetzungen für eine sichere Kommunikation nur unzureichend erfüllten. Allerdings können gezielte Nachbesserungen das Sicherheitsniveau der Web-Angebote im Landkreis Donau-Ries erhöhen. Um die Entwicklung in diesem Bereich weiter beobachten zu können, werden die hier vorgestellten Untersuchungen zu einem späteren Zeitpunkt wiederholt und den aktuellen Ergebnissen gegenübergestellt.

Quellenverzeichnis

[1] FdWB, Studie des FdWB von 2.500 Webseiten 2020, https://fdwb.de/studie-des-fdwb-von-2-500-webseiten-2020/

[2] SSLyze, SSLyze documentation, https://nabla-c0d3.github.io/sslyze/documentation/

[3] BSI, TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 - Verwendung von Transport Layer Security (TLS), aktuelle Version verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

[4] BSI, TR-02103, X.509 Zertifikate und Zertifizierungspfadvalidierung, aktuelle Version verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02103/tr02103_node.html

[5] BSI, Sicherheit von Webanwendungen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/WebSec/WebSec.pdf?__blob=publicationFile&v=1

[6] BSI, TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, aktuelle Version verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

[7] BSI, BSI-Standards zur Internet-Sicherheit (Isi-Reihe), Sicheres Bereitstellen von Web-Angeboten (Isi-Webserver), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/ISI-Reihe/isi-reihe_node.html

[8] BSI, Hilfsdokument zum „Mindeststandard des BSI zur Verwendung von Transport Layer Security V2.2“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Hilfsdokument_Mindeststandard_BSI_TLS_Version_2_2.pdf?__blob=publicationFile&v=4

[9] IETF, Deprecating TLS 1.0 and TLS 1.1, https://datatracker.ietf.org/doc/rfc8996/

[10] siwecos.de, SIWECOS: Jede zweite Firmenwebseite ist gefährdet, https://siwecos.de/presse/115-siwecos-jede-zweite-firmenwebseite-ist-gefaehrdet

[11] blog.mozilla.org, Reducing TLS Certificate Lifespans to 398 Days, https://blog.mozilla.org/security/2020/07/09/reducing-tls-certificate-lifespans-to-398-days/

[12] support.apple.com, About upcoming limits on trusted certificates, https://support.apple.com/en-us/HT211025

[13] chromium.googlesource.com, Certificate Lifetimes, https://chromium.googlesource.com/chromium/src/+/HEAD/net/docs/certificate_lifetimes.md

[14] letsencrypt.org, Let's Encrypt, https://letsencrypt.org/

IMPRESSUM UND KONTAKT

Herausgeber und v. i. S. d. P.
Prof. Dr. Gordon Thomas Rohrmair,
Präsident der Hochschule Augsburg

Projektleitung
Prof. Dr.-Ing. Dominik Merli,
Leiter HSA_innos
und TTZ Data Analytics

Autoren
Florian Ernst,
Fabian Bley,
Benjamin Kienle

Redaktion
Alexander Lehner
alexander.lehner@hs-augsburg.de

Kontakt
Hochschule Augsburg
University of Applied Sciences
An der Hochschule 1
86161 Augsburg
Tel. +49 821 5586-0
Fax +49 821 5586-3222
info@hs-augsburg.de
www.hs-augsburg.de

Institut für innovative Sicherheit (HSA_innos)
Prof. Dr.-Ing Dominik Merli
Am Technologiezentrum 8
86159 Augsburg
www.hsainnos.de
info@hsainnos.de

Technologietransferzentrum Data Analytics
Prof. Dr. Björn Steven Häckel
Äbtissin-Gunderada-Straße 4
86609 Donauwörth
www.ttz-data-analytics.de
ttz-don@hs-augsburg.de

Gestaltung
wppt : kommunikation gmbh
Gesellschaft für visuelle Kultur
Treppenstraße 17 – 19
42115 Wuppertal
Rob Fährmann
Tel. +49 202 42966-0
Fax +49 202 42966-29
direkt@wppt.de
www.wppt.de

Druck
Druckerei Hans Hitzegrad
GmbH & Co. KG
Friedrich-Ebert-Straße 102
42117 Wuppertal
Auflagenhöhe: 750 Exemplare

Hochschule Augsburg
University of Applied Sciences
An der Hochschule 1
86161 Augsburg
info@hs-augsburg.de
www.hs-augsburg.de

Institut für innovative
Sicherheit (HSA_innos)
Am Technologiezentrum 8
86159 Augsburg
www.hsainnos.de
info@hsainnos.de

Technologietransferzentrum (TTZ)
Data Analytics
Äbtissin-Gunderada-Straße 4
86609 Donauwörth
www.ttz-data-analytics.de
ttz-don@hs-augsburg.de