Bayerisches Landesamt für
Datenschutzaufsicht

Ansbach, den 10. Oktober 2017

Pressemitteilung

BayLDA prüft Verschlüsselung von Webseiten

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) startet seine „Cybersicherheitsinitiative zum Schutz personenbezogener Daten". Dazu wird als erster Baustein ein neuer Online-Service angeboten, über den die HTTPS-Verschlüsselung einer Webseite zur Überprüfung gemeldet werden kann.

Aktuelle Gefährdungslage

Cyberangriffe haben in den vergangenen Jahren spürbar zugenommen. Dafür gibt es verschiedene Gründe, wobei der Profit durch den gezielten Verkauf personenbezogener Daten im Darknet als Hauptmotivation relativ weit oben steht. Für Cyberkriminelle ist dieses „Geschäft" rentabel, für Unternehmen dagegen der blanke Horror: schließlich drohen durch solche Angriffe einerseits empfindliche finanzielle Verluste, andererseits aber auch nachhaltige Imageschädigungen, die eine Abwanderung von Kunden zur Folge haben können. Für die Betroffenen sind neben finanziellen Schäden auch die Verletzung ihrer Persönlichkeitsrechte, wie z. B. Rufschädigung oder Diskriminierung, zu befürchten.

Als Datenschutzaufsichtsbehörde ist das BayLDA bei der Aufarbeitung solcher Vorfälle bereits heute involviert: Nach § 42a Bundesdatenschutzgesetz (BDSG) besteht eine Meldepflicht von Unternehmen über Sicherheitsvorfälle, wenn sensible Daten betroffen sind (z. B. Bank- oder Gesundheitsdaten) und gleichzeitig den betroffenen Personen schwerwiegende Beeinträchtigungen drohen. Während früher dem BayLDA im Rahmen dieser sog. Datenpannenmeldungen meist die Fehlversendung vertraulicher Unterlagen oder der Verlust von Datenträgern mitgeteilt wurde, wird die Behörde mittlerweile vermehrt auch mit Meldungen von Hacking-Angriffen konfrontiert. So melden Unternehmen, dass Kundendaten aus dem Webshop gestohlen wurden oder Ärzte, dass sie aufgrund eines Verschlüsselungstrojaners nicht auf Patientendaten zugreifen können. Vorfälle, bei denen es hunderttausende Betroffene gibt oder ein sehr hoher finanzieller Schaden entsteht, sind keine Seltenheit mehr.

Cybersicherheitsinitiative zum Schutz personenbezogener Daten

Gerade aufgrund der gestiegenen Gefährdungslage im Internet und dem Ausblick, dass eine baldige Besserung hierbei nicht erkennbar ist, stärkt das BayLDA seinen Fokus auf Maßnahmen zur Cybersicherheit für bayerische Unternehmen, damit diese personenbezogene Daten zeitgemäß, angemessen und wirksam vor den täglichen Gefahren im digitalen Zeitalter besser schützen. Das BayLDA will künftig insbesondere durch flächendeckende automatisierte Prüfungen Schwachstellen und Sicherheitslücken aufzeigen, um dadurch Unternehmen in Bayern zu sensibilisieren und, sollte es notwendig sein, auch dazu zu bewegen, sicherheitsrelevante Themen mit entsprechender Ernsthaftigkeit zu begegnen. Letztendlich drohen ab Mai 2018 durch die Datenschutz-Grundverordnung (DS-GVO) bei Verstößen Bußgelder in empfindlicher Größenordnung: Bis zu 10 Millionen Euro oder bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des Unternehmens (je nachdem, welcher Betrag höher ist) können verhängt werden.

Anschrift
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

Telefon +49 (0) 981 53 1300
Telefax +49 (0) 981 53 98 1300
E-Mail presse@lda.bayern.de
Webseite www.lda.bayern.de

Öffentliche Verkehrsmittel
Bushaltestellen Schlossplatz
oder Bahnhof der Stadt- und
Regionallinien

Online-Service „HTTPS-Check“

Als ersten Schritt dieser Cybersicherheitsinitiative prüft das BayLDA die Verschlüsselung von Webseiten bayerischer Anbieter (Details zum Ablauf der Prüfung siehe Anhang). Die Erfahrung des BayLDA zeigt bislang, dass Webserver von Unternehmen nicht immer entsprechend dem Stand der Technik betrieben werden. Das Hauptproblem liegt dabei im Fehlen eines Zertifikats oder einer nicht ausreichenden HTTPS-Konfiguration – was dazu führt, dass Kundendaten unverschlüsselt oder schwach verschlüsselt durch das Internet zum Zielserver übertragen und letztendlich abgegriffen werden können. Zwar können auch Daten, die entsprechend dem Stand der Technik verschlüsselt sind, abgefangen werden – jedoch ist bei diesen ein „Knacken“ massenhafter Daten ohne unverhältnismäßigen Aufwand kaum möglich.

Neben der Prüfung einiger von uns ausgewählter Webseiten bietet der neue Online-Service des BayLDA erstmals die Möglichkeit an, dass konkrete Webseiten zur Überprüfung mitgeteilt werden. Sowohl Unternehmen, die Ihre eigene Webseite prüfen lassen wollen, als auch Bürger, die bestimmte Internet-Dienste prüfen lassen möchten, können die jeweilige URL auf der Homepage des BayLDA in ein dafür vorgesehenes Formularfeld eingeben. Unternehmen, die ihre eigene Webseite eingegeben haben, erhalten ein schriftliches Feedback mit dem Ergebnis der Prüfung. Bürger, die eine Webseite von Dritten nennen, bekommen keine persönliche Rückmeldung, können allerdings sicher sein, dass wir die Einhaltung der Mindestanforderungen an die HTTPS-Verschlüsselung bei den gemeldeten Webseiten sicherstellen werden. Falls die HTTPS-Verschlüsselung der Webseite den gesetzlichen Anforderungen nicht entspricht, werden die betroffenen Unternehmen zur Nachbesserung aufgefordert und als letztes Mittel auch per Anordnung dazu gezwungen. Der **HTTPS-Check** kann über folgenden Link auf der Webseite des BayLDA angestoßen werden:

www.lda.bayern.de/de/httpscheck.html

Andreas Sachs, Vertreter des Präsidenten und gleichzeitig Leiter des Referats für IT-Sicherheit und technischen Datenschutz im BayLDA, äußert sich zur Cybersicherheitsinitiative und dem neuen Online-Service wie folgt:

> *„Prävention bleibt auch im technischen Datenschutzumfeld das A und O. Während man in der Vergangenheit das Gefühl hatte, gegen Windmühlen ankämpfen zu müssen, stellen wir jetzt zumindest fest, dass „Sicherheit“ in den Köpfen angekommen ist. Der nächste Schritt ist nun, aufzuzeigen, an welchen Stellen die Unternehmen konkret anpacken müssen. Wir wollen auch künftig unseren Teil dazu beitragen, dass die Anzahl kritischer Vorfälle in Bayern möglichst gering bleibt und im Zweifelsfall, wenn es doch dazu kommt, dass der Schaden durch eine gezielte Aufarbeitung minimiert wird. Sollten wir jedoch bei unseren Prüfungen auf „schwarze Schafe“ treffen, die sich weigern, den gesetzlichen Anforderungen an den Datenschutz nachzukommen, werden wir diese mit Anordnungen oder Bußgeldern zwingen, den Grundrechtsschutz ihrer Beschäftigten, Kunden und/oder Interessenten zu wahren.“*

Das BayLDA appelliert an alle bayerischen Verantwortlichen, d. h. Unternehmen, Vereine, Verbände, freiberuflich Tätigen usw., die mit personenbezogenen Daten umgehen, das Thema Cybersicherheit ernst zu nehmen. Mit der DS-GVO wird der Gesichtspunkt der Sicherheit der Verarbeitung auch formell bedeutender, sodass es für Unternehmen keinerlei Spielraum gibt, dieses Thema nur stiefmütterlich zu behandeln.

Thomas Kranig
Präsident

Anhang:
Allgemeine Hinweise zum Ablauf der Überprüfung der HTTPS-Verschlüsselung einer Webseite

Ablauf der Überprüfung der HTTPS-Verschlüsselung einer Webseite

1. **Objekt der Prüfung**

   Das BayLDA untersucht sowohl Webseiten, deren URLs eigenständig erhoben wurden, als auch die, die von den Webseitenbetreibern selbst oder von Dritten dem BayLDA mitgeteilt worden sind (z. B. per E-Mail oder über den neuen Online-Service „HTTPS-Check").

2. **Gegenstand der Prüfung**

   Geprüft wird, ob die Webseiten über eine ausreichende HTTPS-Verschlüsselung verfügen, um den Datentransfer zwischen dem Browser des Nutzers und dem Internet-Server des Anbieters abzusichern. Dies gilt besonders für Webseiten, bei denen Kontakt- und Zahlungsdaten eingegeben werden können (z. B. Online-Shops), sowie für Webseiten von Unternehmen, die ein Kontaktformular als mögliches Kommunikationsmedium anbieten. Darüber hinaus kann in Einzelfällen auch bei anderen Webseiten eine HTTPS-Verschlüsselung erforderlich sein, da weitere Nutzungsdaten verarbeitet werden.

3. **Durchführung der Prüfung**

   Anhand eines eigenhändig erstellten Prüfskripts auf Basis der OpenSSL-Bibliothek werden die Webseiten automatisiert daraufhin überprüft, ob die HTTPS-Transportverschlüsselung dem Stand der Technik entspricht. Unter anderem werden folgende Kriterien dabei berücksichtigt:

   - Priore Verwendung von Perfect Forward Secrecy (PFS)
   - Kein Einsatz veralteter Verschlüsselungsprotokolle (SSL2, SSL3)
   - Zertifikate mit mindestens 2048-Bit Schlüssellänge
   - HTTP Strict Transport Security (HSTS) zur Eindämmung der Risiken von Man-in-the-Middle-Angriffen
   - Keine Verwendung von unsicheren Kryptoalgorithmen (z. B. RC4, SHA-1)

4. **Umgang mit dem Ergebnis der Prüfung**

   Alle Unternehmen, deren Webseiten von uns überprüft wurden, erhalten einen kurzen automatisch generierten Prüfbericht. Soweit die Webseiten über eine ausreichende Verschlüsselung verfügen, wird dies entsprechend schriftlich bestätigt. Sollten jedoch Mängel durch die Prüfung erkannt werden, so werden diese dem Betreiber mit der Aufforderung mitgeteilt, innerhalb einer Frist die erforderlichen Maßnahmen zur Verschlüsselung umzusetzen. Sofern Betreiber von Webseiten ohne ausreichende Begründung der Verpflichtung, eine angemessene Verschlüsselung vorzusehen, nicht nachkommen, wird das BayLDA durch eine entsprechende Anordnung die Betreiber verpflichten, die Verschlüsselung zu implementieren und, falls dieser Anordnung nicht nachgekommen wird, gegebenenfalls ergänzend einen Bußgeldbescheid gegen den Verantwortlichen erlassen.

5. **Weitere Schritte im Rahmen der „Cybersicherheitsinitiative zum Schutz personenbezogener Daten"**

   Die Überprüfung der Verschlüsselung Webseiten bayerischer Anbieter ist der erste Baustein in einer geplanten Serie von Prüfszenarien. Das BayLDA beabsichtigt beispielsweise als weitere Schritte zu prüfen, ob über das Internet erreichbare Server mit aktuellen Softwareversionen ausgestattet sind oder ob verwundbare Systeme betrieben werden (Patch-Management). Informationen zu den weiteren Prüfungen werden auf der Webseite des BayLDA unter www.lda.bayern.de veröffentlicht.

Anschrift
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

Telefon +49 (0) 981 53 1300
Telefax +49 (0) 981 53 98 1300
E-Mail presse@lda.bayern.de
Webseite www.lda.bayern.de

Öffentliche Verkehrsmittel
Bushaltestellen Schlossplatz
oder Bahnhof der Stadt- und
Regionallinien