BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

Pressemitteilung

9. September 2014

Datenschutzprüfung bei Mailservern bayerischer Unternehmen

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat Anfang September 2014 bei insgesamt 2.236 bayerischen Unternehmen das Sicherheitsniveau der eingesetzten Mailserver automatisiert überprüft. 772 Unternehmen genügten dabei den gestellten datenschutzrechtlichen Anforderungen nicht und wurden deshalb vom BayLDA schriftlich aufgefordert, ihre Mailserver an den Stand der Technik anzupassen.

Allgemein bekannt ist die Tatsache, dass das Versenden unverschlüsselter E-Mails vom Grad der Geheimhaltung wie das Verschicken einer Postkarte bewertet wird. Jeder, der die Karte zu Gesicht bekommt, kann ohne größeren Aufwand den Inhalt lesen, auswerten oder sogar ändern. Dass ein solches Mitlesen unverschlüsselter E-Mails nicht nur für Geheimdienste problemlos möglich ist, ist nicht erst seit den Enthüllungen von Edward Snowden bekannt, aber sicherlich mehr in das Bewusstsein der Allgemeinheit gedrungen. Aus diesem Grund sind Unternehmen darauf hinzuweisen, dass sie nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) verpflichtet sind, im Rahmen der Zugangs-, Zugriffs- und Weitergabekontrolle Verschlüsselungsverfahren in angemessenem Umfang bei den von Ihnen eingesetzten Mailservern nach dem Stand der Technik zu verwenden.

Verschlüsselung mit STARTTLS und Perfect Forward Secrecy

Wenn eine E-Mail verschickt werden soll, „handeln“ die beteiligten Mailserver zunächst einen Standard für die Übertragung der Nachricht aus, bevor die E-Mail tatsächlich verschickt wird. Das heißt, die Mailserver fragen, sofern sie entsprechend konfiguriert sind, jeweils bei dem anderen nach, ob eine Transport-Verschlüsselung (Transport Layer Security, kurz TLS) unterstützt wird und übertragen dann die E-Mail mit dem bestmöglichen Grad der Verschlüsselung. Mailserver von Unternehmen müssen deshalb das hierbei angewandte Verfahren **STARTTLS** zur Verschlüsselung unterstützen, damit eine Transport-Verschlüsselung bei der Übermittlung von E-Mails überhaupt ermöglicht werden kann. Zusätzlich ist das so genannte **Perfect Forward Secrecy** einzusetzen, damit selbst bei unrechtmäßiger Erlangung eines geheimen Schlüssels der mit TLS verschlüsselte E-Mailverkehr nicht nachträglich entschlüsselt werden kann.

Briefanschrift
Postfach 6 06, 91511 Ansbach

Frachtanschrift
Promenade 27, 91522 Ansbach

Dienstgebäude
Promenade 27
(Schloss)

Telefon 0981 53-1300
Telefax 0981 53-5300
E-Mail presse@lda.bayern.de
Internet www.lda.bayern.de

Öffentliche Verkehrsmittel
Bushaltestellen Schlossplatz
oder Bahnhof der Stadt- und
Regionallinien

Durch diese Art der Verschlüsselung können zwar gezielte Angriffe von Geheimdiensten oder Cyberkriminellen nicht gänzlich ausgeschlossen werden - das problemlose Mitlesen und Auswerten des gesamten E-Mailverkehrs wird damit aber deutlich erschwert. Es wird jedoch ausdrücklich darauf hingewiesen, dass eine Transportverschlüsselung durch STARTTLS keinen Ersatz für eine Ende-zu-Ende Verschlüsselung (z. B. mit PGP) darstellt, sondern als zusätzlicher Baustein zur Erhöhung der Kommunikationssicherheit zu sehen ist.

Der Aufwand für Unternehmen, diese Maßnahmen zur Erhöhung der Sicherheit ihrer Mailserver umzusetzen, ist im Allgemeinen als relativ gering anzusehen. Hauptsächlich gilt es die Konfiguration der Mailserver an den Stand der Technik anzupassen. Gegebenenfalls müssen zusätzlich TLS-Zertifikate, sofern diese noch nicht vorhanden sind, von einer vertrauenswürdigen Stelle erworben werden.

Heartbleed-Lücke bei 44 Unternehmen

Im Zuge dieser datenschutzrechtlichen Onlineprüfung, die auf die Sicherheitsaspekte STARTTLS und Perfect Forward Secrecy fokussiert war, hat das BayLDA auch festgestellt, dass bei 44 von bayerischen Unternehmen eingesetzten Mailservern die so genannte Heartbleed-Lücke besteht. Dabei handelt es sich um ein sehr kritisches Problem bei der Nutzung bestimmter Versionen der Softwarebibliothek OpenSSL. Bei Vorhandensein dieser Sicherheitslücke besteht die Gefahr, dass Unbefugte über das Internet ohne Probleme Fragmente der E-Mail-Kommunikation - vom Nutzer unbemerkt - abgreifen oder sogar den privaten Schlüssel auslesen können. Durch ständig wiederholte Nachfragen könnte aus diesen Fragmenten der wesentliche Inhalt des Mailverkehrs erschlossen werden. Bereits im April 2014 wurde in den Medien umfangreich über diese Heartbleed-Sicherheitslücke informiert, so dass das BayLDA eigentlich davon ausgegangen ist, dass diese Schwachstelle nicht mehr bestehen dürfte.

Informationen auch unter www.lda.bayern.de/onlinepruefung/

Das BayLDA hat in seinem Schreiben die betroffenen Unternehmen über das Ergebnis der Prüfung informiert sowie umfassende Hinweise zur rechtlichen und technischen Grundlage dieser Onlineprüfung mitgesandt. Zusätzlich informiert das BayLDA auf seiner Webseite (http://www.lda.bayern.de/onlinepruefung/) darüber, auf welcher Basis die Prüfung durchgeführt wurde und welche Schritte angeschriebene Unternehmen durchführen müssen, um den gesetzlichen Anforderungen gerecht zu werden. Hierbei bietet das BayLDA auch einen umfassenden FAQ-Bereich mit Antworten zu den häufig gestellten Fragen an, der allen Betroffenen und Interessierten zur Verfügung steht. Darüber hinaus können sich Unternehmen mit konkreten Fragen, die über die allgemeinen Informationen hinausgehen, über die E-Mail-Adresse onlinepruefung@lda.bayern.de an die Aufsichtsbehörde wenden.

Vollzug einer Entschließung der deutschen Datenschutzbehörden

Das BayLDA hat mit dieser Aktion eine Entschließung der 87. Konferenz der Datenschutzbehörden des Bundes und der Länder vom 27. März 2014 (http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/87_DSKMenschenrechteElektrischeKommunikation.html?nn=409240) vollzogen, in der u. a. sichere Verschlüsselung beim Transport von Daten als wesentliches Element für den Datenschutz gefordert wurde.

Thomas Kranig
Präsident