Bayerischer Landtag

17. Wahlperiode

14.08.2014 17/2511

Schriftliche Anfrage

des Abgeordneten **Markus Rinderspacher SPD**
vom 28.04.2014

Konsequenzen aus dem Heartbleed-Bug

Ein kleiner Fehler in einer weitverbreiteten freien Verschlüsselungssoftware hat dafür gesorgt, dass Tausende Webserver ausgerechnet dann bei Datenübermittlungen angreifbar waren, wenn die Kommunikation aus schutzwürdigen Gründen (private Schlüssel von X.509-Zertifikaten, Benutzernamen und Passwörter) kryptografiert hätte stattfinden sollen.

Die sogenannte Heartbleed-Sicherheitslücke vom April 2014 belegt: Die Sicherheit verschlüsselten Datenverkehrs im Internet darf nicht darauf angewiesen sein, dass ehrenamtlich arbeitende Experten einer Stiftung, die sich über Spenden zu finanzieren versucht, keinen Schnitzer machen.

Deshalb frage ich die Bayerische Staatsregierung:

1. Welche Vorgaben seitens des CIO Bayerns gibt es zur Nutzung und Überprüfung von SSL-Verschlüsselungssoftware und zum Einsatz von OpenSSL in Behörden und staatlichen Stellen?

2. Wie viele Webserver staatlicher Stellen und Behörden in Bayern und wie viele Dienstleister, die in behördlichem Auftrag Onlineangebote im Web betreiben, waren vom Heartbleed-Bug betroffen?

3. Haben staatliche Stellen, die die freie Verschlüsselungstechnik der OpenSSL Software Foundation direkt oder über Dienstleister nutzen, finanziell zu deren Weiterentwicklung beigetragen?

4. Wie bewertet die Staatsregierung die Klage der OpenSSL Software Foundation über die mangelnde Unterstützung vor allem durch Konzerne und Regierungen, die die kostenfrei erhältliche Software für ihre Server zwar nutzen, aber die Entwickler nicht honorieren?

5. Wie steht die Staatsregierung zu Forderungen, sensible und sicherheitskritische Softwareentwicklungen wie Verschlüsselungstechniken zum Schutz der Daten von Bürgerinnen und Bürgern unter dem Gedanken staatlicher Vorsorge und Gefahrenabwehr künftig besser zu unterstützen?

6. Wie steht die Staatsregierung zu Forderungen, dass staatliche Stellen die Bürgerinnen und Bürger unmittelbar nach aufgedeckten schwerwiegenden IT-Sicherheitslücken wie dem Heartbleed-Bug besser als bisher über Gefahrenquellen für ihre Datensicherheit informieren und Handlungsempfehlungen geben?

7. In welchem Umfang und zu welchen Zwecken wird im Bereich staatlicher Stellen und Behörden in Bayern Open-Source-Software eingesetzt?

8. Wie steht die Staatsregierung zu einer besseren Förderung von Open-Source-Software im Bereich staatlicher Stellen und Behörden in Bayern?

Antwort

des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat
vom 30.06.2014

1. Welche Vorgaben seitens des CIO Bayerns gibt es zur Nutzung und Überprüfung von SSL-Verschlüsselungssoftware und zum Einsatz von OpenSSL in Behörden und staatlichen Einrichtungen?

Die Nutzung von SSL/TLS im Bayerischen Behördennetz (BYBN) ist seit 2006 in der IT-Sicherheitsrichtlinie BayITSiR-11 geregelt. OpenSSL wird hier nicht explizit als SSL-Verschlüsselungssoftware gefordert. Je nach Nutzungsart wird eine entsprechende Zertifizierung gefordert, die die fehlerfreie Implementierung der kryptografischen Funktionen sicherstellen soll.

2. Wie viele Webserver staatlicher Stellen und Behörden in Bayern und wie viele Dienstleister, die in behördlichem Auftrag Onlineangebote im Web betreiben, waren vom Heartbleed-Bug betroffen?

Der Betrieb von Webservern im Bayerischen Behördennetz ist in der IT-Sicherheitsrichtlinie (BayITSiR-02) geregelt. Der Zugriff auf diese Webserver aus dem Internet ist nur über einen einzigen, speziell abgesicherten Zugang (sog. Reverse-Proxy) gestattet. Dieser Reverse-Proxy war nicht von dem Heartbleed-Bug betroffen. In Folge dessen hat sich der Heartbleed-Bug auch nicht auf Webserver im Bayerischen Behördennetz ausgewirkt.

Von den außerhalb des Bayerischen Behördennetzes betroffenen Webservern staatlicher Stellen und Behörden war ein Webserver (ELSTER) betroffen. Ein unberechtigter Zugriff auf personenbezogene oder steuerlich relevante Daten der Bürger war zu keinem Zeitpunkt möglich. Es war lediglich das Informationsangebot unter www.elster.de betroffen. Alle notwendigen Maßnahmen wurden sofort nach Bekanntwerden durchgeführt. Das Elster-Online-Portal, das elektro-

nische Finanzamt der Steuerverwaltung unter www.elsteronline.de, sowie das PC-Programm Elster-Formular waren nicht betroffen. Die Bürger wurden über einen Blog-Eintrag auf www.elster.de zeitnah informiert (http://blog.elster.de/wordpress/?p=767).

3. Haben staatliche Stellen, die die freie Verschlüsselungstechnik der OpenSSL Foundation direkt oder über Dienstleister nutzen, finanziell zu deren Weiterentwicklung beigetragen?

Bei OpenSSL handelt es sich um einen Software-Baustein, der als einer von vielen Bestandteilen in – in der Regel kostenpflichtige – Softwareprodukte verschiedenster Hersteller Verwendung findet. Setzt die Staatsregierung solche Produkte ein, so erfolgt der Einsatz im Rahmen entsprechender Lizenz- und Wartungsverträge. Es wird davon ausgegangen, dass die OpenSSL einsetzenden Hersteller aus ihren Einnahmen aus Lizenz- und Wartungsverträgen die OpenSSL-Foundation angemessen unterstützen. Nach unseren Informationen haben keine staatlichen Stellen direkt die freie Verschlüsselungstechnik der OpenSSL Foundation finanziell unterstützt.

Eine Unterstützung und aktive Beteiligung an Open Source Projekten durch den Freistaat Bayern erfolgt im Rahmen seiner Mitgliedschaft in der Open Source Business Alliance.

4. Wie bewertet die Staatsregierung die Klage der OpenSSL-Foundation über die mangelnde Unterstützung vor allem durch Konzerne und Regierungen, die die kostenfrei erhältliche Software für ihre Server nutzen, aber die Entwicklung nicht honorieren?

Wie in der Antwort zu Frage 3 ausgeführt, handelt es sich bei OpenSSL um einen Software-Baustein, der in konkreten Softwareprodukten Verwendung findet. Eine Unterstützung der OpenSSL-Foundation sollte deshalb durch die entsprechenden Softwarehersteller erfolgen. Ob und in welchem Umfang dies der Fall ist, kann durch die Staatsregierung nicht beurteilt werden.

5. Wie steht die Staatsregierung zu Forderungen, sensible und sicherheitskritische Softwareentwicklungen wie Verschlüsselungstechniken zum Schutz der Daten von Bürgerinnen und Bürgern unter dem Gedanken staatlicher Vorsorge und Gefahrenabwehr künftig besser zu unterstützen?

Den Bürgerinnen und Bürgern steht eine Vielzahl an Technologien – sowohl Open-Source- als auch kommerzielle Produkte – zum Schutz ihrer persönlichen Daten in den unterschiedlichsten Anwendungsfällen zur Verfügung. Wie aktuelle Studien zeigen, werden diese allerdings noch zu wenig genutzt. Daher liegt der Fokus der Bayerischen Staatsregierung zum Schutz der Daten von Bürgerinnen und Bürgern unter dem Gedanken staatlicher Vorsorge im Bereich der Sensibilisierung, da im bewussten Umgang mit IT-Sicherheit eindeutig das größte Potenzial zur Erhöhung der Datensicherheit liegt.

Zudem unterstützt die Bayerische Staatsregierung die IT-Sicherheitsforschung (z. B. Grundlagenforschung zu Kryptografie und ausfall- und angriffssicheren Protokollen) auch finanziell. Den Schwerpunkt bildet hier der Ausbau des Fraunhofer-Instituts für angewandte und integrierte Sicherheit (AISEC) zu einem Sicherheitskompetenzzentrum von internationaler Bedeutung.

6. Wie steht die Staatsregierung zu Forderungen, dass staatliche Stellen die Bürgerinnen und Bürger unmittelbar nach aufgedeckten schwerwiegenden IT-Sicherheitslücken wie dem Heartbleed-Bug besser als bisher über Gefahrenquellen für ihre Datensicherheit informieren und Handlungsempfehlungen geben?

Neben einzelnen Initiativen mit staatlicher Beteiligung, wie z. B. Deutschland sicher im Netz e. V. (https://www.sicher-im-netz.de), leistet das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale staatliche Stelle für IT-Sicherheit sehr gute Arbeit. Mit dem Bürger-CERT (https://www.buerger-cert.de/) und der Website „BSI für Bürger“ (https://www.bsi-fuer-buerger.de) stehen exakt die geforderten Instrumente zur Bürgerinformation zur Verfügung (z. B. Newsletter).

Die geplante Homepage „Initiative Cybersicherheit Bayern“ (http://www.cybersicherheit.bayern.de) wird dieses bestehende Angebot um konkrete bayerische Ansprechpartner für unterschiedliche Bedarfsträger ergänzen.

7. In welchem Umfang und zu welchen Zwecken wird im Bereich staatlicher Stellen und Behörden in Bayern OpenSource-Software eingesetzt?

Open-Source-Software spielt in der Bayerischen Staatsverwaltung eine wichtige Rolle. Sie wird basierend auf dem Betriebssystem Linux und der Bürosoftware OpenOffice in der Staatsverwaltung an ca. 3600 Arbeitsplätzen eingesetzt, insbesondere im Bereich der Vermessungsverwaltung. Darüber hinaus hat sich Open Source Software in den staatlichen Rechenzentren vor allem im Bereich der Server- und Infrastruktur-Systeme bewährt.

8. Wie steht die Staatsregierung zu einer besseren Förderung von Open-Source-Software im Bereich staatlicher Stellen und Behörden in Bayern?

Wie bereits zu Frage 3 ausgeführt, erfolgt eine Unterstützung und aktive Beteiligung an Open-Source-Projekten durch den Freistaat Bayern im Rahmen seiner Mitgliedschaft in der Open-Source-Business Alliance (OSB). Die OSB ist Europas größtes Netzwerk von Unternehmen und Organisationen, die Open Source Software entwickeln, darauf aufbauen oder sie anwenden. Ziel der OSB ist es, Open-Source-Software und andere Formen offener Zusammenarbeit aktiv zu fördern.