Mit SSL-Analyse besserer Schutz für staatliche IT

bfg:Herr Kleffel, das LSI wurde vom Finanzministerium beauftragt, eine Analyse von SSL-Verbindungen zu pilotieren. Was kann man sich darunter vorstellen?

Kleffel: Am zentralen Übergang des Behördennetzes zum Internet wird vom IT-DLZ ein sogenannter „Forward Proxy" zum Schutz und zur Sicherstellung des Betriebs im gesamten Bayerischen Behördennetz (BYBN) eingesetzt. Jeder Kontakt in das Internet aus dem BYBN, z.B. der Aufruf von www.google.de, läuft über diese Infrastruktur. Dabei werden permanent sicherheitstechnische Analysen für unverschlüsselten Datenverkehr durchgeführt. Allerdings bauen die meisten Webseiten mittlerweile nur noch verschlüsselte SSL-Verbindungen auf, die am Forward Proxy nicht analysiert werden können. Das hat zur Folge, dass unsere Sicherheitsmaßnahmen bereits heute bei rund 78 Prozent des Datenverkehrs nicht oder nur noch eingeschränkt wirken – Tendenz weiter klar steigend.

Bei der SSL-Analyse handelt sich um ein Verfahren, bei dem der SSL-verschlüsselte Datenverkehr am Forward Proxy in zwei getrennte verschlüsselte Verbindungen aufgeteilt wird und somit in Echtzeit automatisiert analysiert werden kann. Auf diese Weise stehen auch für verschlüsselten Datenverkehr sämtliche sicherheitstechnischen Maßnahmen zum Schutz der staatlichen IT-Infrastruktur zur Verfügung. Zugriffe auf BYBN-interne Seiten, zum Beispiel auf Intranetangebote, werden nicht analysiert.

bfg: Was bedeutet das für die Beschäftigten, sollte dieses Verfahren in der Finanzverwaltung flächendeckend eingesetzt werden?

Kleffel: Das Verfahren bringt dem BYBN und damit natürlich auch für jeden Beschäftigten ein höheres Maß an Sicherheit. Für die Nutzer ändert

LSI-Chef Daniel Kleffel

Mit explodierender digitaler Vernetzung aller nur denkbarer Informationen und weiter steigender Komplexität der IT-Systeme steigt die Gefahr von Cyberangriffen ständig an. Dass das keine blinde Angstmacherei ist, zeigt der tägliche Blick in die Nachrichten. Datendiebstahl in großem Maß ebenso wie tage- oder wochenweise ausgefallene IT-Systeme sind auch in sehr großen Firmen an der Tagesordnung. Um das Schutzniveau der öffentlichen Verwaltung in Bayern an die wachsenden Gefahren anzupassen, wurde das Landesamt für Sicherheit in der Informationstechnik als die IT-Sicherheitsbehörde des Freistaats Bayern gegründet. Aufgaben des LSI sind neben dem aktiven Schutz der staatlichen IT-Systeme die Beratung von Kommunen, öffentlichen Unternehmen als Betreiber kritischer Infrastrukturen und der Staatsverwaltung an sich. Über die BayernLabs wird ein Beratungsangebot für Bürger in allen Teilen Bayerns aufgebaut. Sitz des Landesamtes ist Nürnberg mit den beiden Außenstellen in Würzburg und Bad Neustadt a. d. Saale. Als noch junges Landesamt wächst das LSI kontinuierlich, um seine Aufgaben bestmöglich zu erfüllen. Im Endausbau soll es bis auf 200 IT-Sicherheitsexperten wachsen. Unverzichtbar ist eine enge und reibungslose Zusammenarbeit mit dem IT-DLZ und dem RZ-Nord unter dem Dach des Finanzministeriums. Eine enge, von sehr hohem Vertrauern geprägte Zusammenarbeit der Amtsleitung mit dem Personalrat, der im letzten Sommer erstmalig gewählt wurde, sichert optimale Arbeitsbedingungen für die Kolleginnen und Kollegen am LSI.

Zahlreiche Fachprojekte laufen am LSI, die sämtlich das Ziel eines noch besseren Schutzes der staatlichen IT haben. Eines davon – die SSL-Analyse – wird im nebenstehenden Interview näher beleuchtet.

sich mit der Einführung des Verfahrens nichts: Sie können weiterhin wie bisher Webseiten aufrufen und Internet-Services nutzen. Von Beginn des Projektes an haben wir in Abstimmung mit dem Bayerischen Landesbeauftragten für den Datenschutz (BayLfD) die datenschutzrechtlichen Aspekte des Verfahrens berücksichtigt und eine Datenschutzfolgeabschätzung durchgeführt. So wird z.B. eine Ausnahmeliste betrieben, in die Internetadressen aufgenommen werden können, die von der SSL-Analyse ausgenommen werden. Das betrifft beispielsweise Seiten für Onlinebanking oder von Krankenversicherungen. Die jeweils aktuelle Ausnahmeliste ist auf www.lsi.bybn.de unter den aktuellen Projekten einsehbar. Weiterhin wird generell beim Aufruf von Internetseiten aus dem Bereich Banking und Health eine Zwischenseite („Coachingseite") eingeblendet, die dem Nutzer die technische Analyse transparent macht.

bfg: Das Sperren der privaten E-Mail-Accounts im Behördennetz wurde ja gerade mit der fehlenden Überprüfungsmöglichkeit seitens der IT bedingt durch die SSL-Verschlüsselung begründet. Eröffnet das neue Verfahren der SSL-Analyse die Möglichkeit, diese Sperrung aufzuheben?

Kleffel: Hierbei muss man grundlegend zwei Mechanismen unterscheiden:

Bei den sogenannten SSL-Verbindungen handelt es sich um eine Transportverschlüsselung. Mit der SSL-Analyse können wir vor allem den Sicherheitsverlust ausgleichen, der mit der stärkeren Verbreitung von SSL-Webseiten einhergeht. Mit der Maßnahme bewahren wir folglich das Sicherheitsniveau. Unter dem Strich entsteht jedoch kein zusätzlicher Schutzmechanismus.

Bei der Verwendung von Webmail ist jedoch auch der Einsatz von Ende-zu-Ende verschlüsselten E-Mails (inkl. Anhängen) mittels gängiger Verfahren wie S/MIME oder PGP möglich und wird von den gängigen Mailanbietern auch sehr einfach anwendbar angeboten. Für diese Art der Verschlüsselung ist eine SSL-Analyse nicht wirksam und würde somit weiterhin ein weitreichendes Sicherheitsrisiko für den Freistaat Bayern darstellen. Deshalb kann aus Sicht des LSI eine Freigabe der Webmailer im BYBN auch mit SSL-Analyse nicht zugestimmt werden. Wir müssen uns vor Augen halten, dass E-Mails nach wie vor Hauptverbreitungsweg für Computerviren sind.

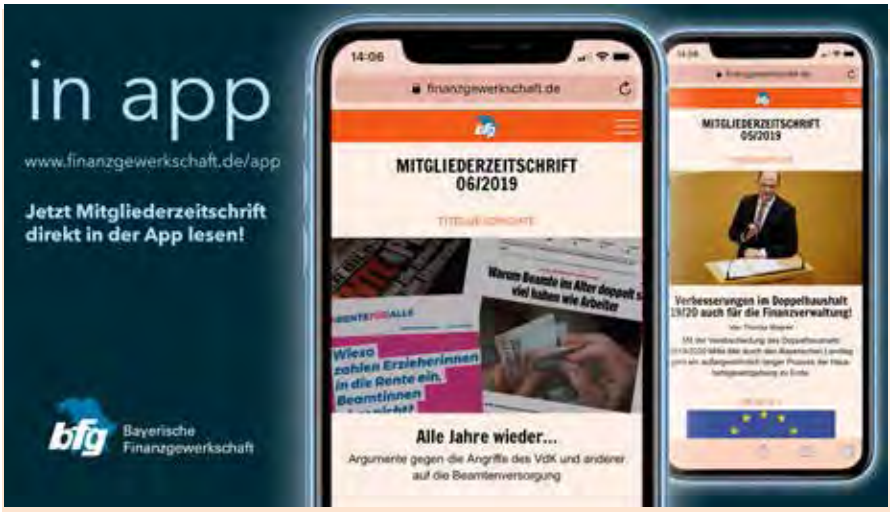
Ich bin dankbar, dass die Personalvertretungen diese leider notwendige Einschränkung in so konstruktiver Weise akzeptieren. Möglicherweise wird das Thema mit der Verbreitung privater Smartphones zunehmend weiter in den Hintergrund treten.

bfg: Erwarten Sie merkliche Auswirkungen auf das Antwort-Zeit-Verhalten durch den Einsatz der SSL-Analyse?

Kleffel: Nein. Aufgrund der eingeplanten Performance-Steigerung der Hardware durch das IT-Dienstleistungszentrum und den bestätigten Erfahrungswerten der bisherigen Pilotierung ist auch weiter mit keinen spürbaren Verzögerungen durch dieses Echtzeit-Verfahren zu rechnen. Am LSI arbeiten wir schon etliche Monate mit dem Verfahren, ohne eine Geschwindigkeitseinschränkung zu spüren.

bfg: Wie sieht der weitere Zeitplan für das Verfahren aus?

Kleffel: Das LSI wurde vom Staatsministerium der Finanzen und für Heimat (StMFH) im letzten Jahr beauftragt, bis Ende des Jahres 2018 die technischen Voraussetzungen zur SSL-Analyse zu schaffen, die rechtlichen Fragestellungen zu klären und in enger Zusammenarbeit mit dem IT-DLZ eine Pilotierung zu realisieren. Diese Vorgaben wurden erfolgreich umgesetzt. Nun erfolgt eine schrittweise Realisierung in weiteren Behörden innerhalb des Finanzressorts bis Ende dieses Jahres, um die SSL-Analyse dann ressortübergreifend in allen weiteren Behörden einzuführen. Klar ist, die SSL-Analyse muss im gesamten BYBN flächendeckend eingeführt werden. Denn auch im Hinblick auf die Abwehr von IT-Sicherheitsgefahren im BYBN gilt das bekannte Sprichwort: „Eine Kette ist nur so stark, wie ihr schwächstes Glied."



Das iPhone bzw. iPad-Betriebssystem IOS in der Version 12.2 und 12.3 erlaubt derzeit keinen Zugriff auf ePub- (iBook) und Mobi-Dokumente (Kindle) über die Web-App. Die Dokumente lassen sich aber im Safari unter der Adresse https://www.finanzgewerkschaft/app ohne Probleme laden. Wir haben jetzt allerdings auch unsere App weiter optimiert und bieten jetzt auch eine „inApp"-Version der bfg-Zeitung an. Bei dieser Version kann die bfg-Zeitung direkt in der App gelesen werden.