**3209/AB**
**vom 17.02.2015 zu 3368/J (XXV.GP)**

BMF
BUNDESMINISTERIUM
FÜR FINANZEN

Frau Präsidentin
des Nationalrates
Doris Bures
Parlament
1017 Wien

Wien, am 11. Februar 2015
GZ. BMF-310205/0281-I/4/2014

Sehr geehrte Frau Präsidentin!

Auf die schriftliche parlamentarische Anfrage Nr. 3368/J vom 17. Dezember 2014 der Abgeordneten Mag. Bruno Rossmann, Kolleginnen und Kollegen beehre ich mich Folgendes mitzuteilen:

Zu 1. und 2.:

Im gegenständlichen Fall handelte es sich nicht um eine Sicherheitslücke in FinanzOnline, sondern um Sicherheitsschwachstellen in zahlreichen Softwareprodukten verschiedenster Hersteller, die am 15. Oktober 2014 bekannt wurden. Betroffen waren vor allem Web-Browser. Die Ursache lag in einer Designschwäche im veralteten Verschlüsselungsprotokoll Secure Socket Layer Version 3 (SSLv3), das bereits 1996 spezifiziert wurde.

Auch wenn es sich nicht um ein Sicherheitsrisiko im Einflussbereich der Betreiber von Webseiten handelte, erging an diese nach Bekanntwerden der Schwachstellen seitens des Österreichischen Computer Emergency Response Teams (CERT.at) die Empfehlung, das alte SSLv3-Protokoll im Sinne der Sicherheit ihrer Benutzerinnen und Benutzer zu deaktivieren und nur mehr das aktuelle Verschlüsselungsprotokoll Transport Layer Security (TLS) zu unterstützen.

Zu 3. bis 7.:

Die Sicherheit der in FinanzOnline verarbeiteten Daten war zu keinem Zeitpunkt gefährdet, zumal FinanzOnline von den gegenständlichen Sicherheitsschwachstellen selbst nicht betroffen war. Aus diesem Grund kann auch ausgeschlossen werden, dass es zu Datenlecks gekommen ist. Das Verschlüsselungsprotokoll wird ausschließlich auf dem Übertragungsweg zwischen Anwender und Server verwendet. Die Daten in den dahinter liegenden Datenbanken von FinanzOnline waren somit nie betroffen.

Zu 8. bis 13.:

Entsprechende Informationen mit folgendem Text wurden zeitnah (innerhalb der folgenden Woche ab Bekanntwerden der Sicherheitsschwachstellen) in den Kommunikationswegen BMF-Homepage, News in FinanzOnline, FinanzOnline Hotline sowie Stakeholder (Interessensvertretungen) geschalten:

„Aufgrund der bekannt gewordenen Sicherheitslücken in Zusammenhang mit dem Verschlüsselungsstandard SSL Secure Socket Layer Protokoll mussten für FinanzOnline rasch Maßnahmen gesetzt werden, um die Sicherheit von Daten und Transaktionen zu gewährleisten.

Die IT der Finanzverwaltung ist nach den strengen Sicherheitsvorschriften ISO 27001 zertifiziert. Die Sicherheit von Daten und Transaktionen hat allerhöchste Priorität. Für die Übertragung von Daten während einer Sitzung wird daher eines der aktuell besten Verschlüsselungssysteme – das Transport Layer Security (TLS) – eingesetzt. Dieses hybride Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet garantiert, dass die Daten verschlüsselt werden, die Identität des Internet-Servers zweifelsfrei bestätigt wird und die Daten vollständig und unverändert übertragen werden.

Aufgrund der aufgetreten Sicherheitsmängel werden daher ältere Verschlüsselungsstandards wie das Secure Socket Layer Protokoll (SSL) ab sofort nicht mehr eingesetzt.

Zusätzlich werden auch ältere Verschlüsselungsalgorithmen (RC4/3DES) aus Sicherheitsgründen nicht mehr unterstützt, da sie nicht mehr den aktuellen Sicherheitsstandards entsprechen.

Dies hat zur Folge, dass der Einstieg in FinanzOnline bei Verwendung des Microsoft Betriebssystems Windows XP oder Windows Server 2003 und dem Webbrowser Internet Explorer Version 8 nicht mehr möglich ist.

Wird Windows XP jedoch mit einem anderen Browser eingesetzt, wie z.B. Mozilla Firefox, Opera, Google Chrome, ist der Einstieg in FinanzOnline nach wie vor möglich.

Wenn das Microsoft Betriebssystem VISTA (Nachfolger von XP) installiert ist, kann noch mit Internet Explorer der Versionen 7, 8 und höher in FinanzOnline eingestiegen werden."

Zu 14. bis 17.:

Im Vorfeld der Deaktivierung des SSLv3-Protokolls wurden verschiedenste Erhebungen und Abwägungen durchgeführt. Zum damaligen Zeitpunkt verwendeten ca. 8 % der Benutzerinnen und Benutzer den Internet Explorer 8.

Konkret verzeichnete FinanzOnline im Monat September 2014 459.000 Einstiege (Logins), davon entfielen lediglich 57 Einstiege auf Benutzerinnen und Benutzer, die das Betriebssystem Windows XP und den Webbrowser Internet Explorer Version 8 verwenden.

Hierzu ist festzuhalten, dass Microsoft den Support für Windows XP und Internet Explorer 8 bereits am 8. April 2014 offiziell eingestellt hat. Sowohl Microsoft als auch zahlreiche Medien warnen seit über einem Jahr davor, die beiden Produkte weiterhin einzusetzen, zumal keine Sicherheitsupdates mehr zur Verfügung gestellt werden und dadurch ein höheres Sicherheitsrisiko besteht.

Auch dem Bundesministerium für Finanzen ist es nicht möglich, Betriebssysteme und Web-Browser weit über ihre Lebensdauer hinaus zu unterstützen und gleichzeitig eine ausreichende Datensicherheit zu gewährleisten. Datensicherheit hat aber Vorrang.

Die FinanzOnline Hotline verzeichnete keinen signifikanten Anstieg von Beschwerden.

Der Bundesminister:

Dr. Schelling

(elektronisch gefertigt)

| | | |
|---|---|---|
| BMF BUNDESMINISTERIUM FÜR FINANZEN | Prüfhinweis | Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://amtssignatur.brz.gv.at/ |
| | Datum/Zeit | 2015-02-17T10:38:29+01:00 |
| Unterzeichner | serialNumber=129971254146,CN=Bundesministerium für Finanzen, C=AT | |
| Signaturwert | fM2Iwd/8tDPLCNFN97IhkAhARbuCxeSZataao+F8l/jM++rIyc69Q8CNlivfnXS uBhdAu3MyewX7QeDk7f36HEmV+9oA/kiUT3N6T3UuIs7+N0mWzzgnAk/f8oByyr 6GM0nM/MbjCqaKi0EmvzA60CfYDsR4FVUUmoWoDQCZn6KZUNEcYfxdT0ib3hF00 BStuF03UXUQe5c4WunNooSJ87dy0PDB9tlRfqy7c/WDvAUyzUj+RZJAV3ngoIex nRAEK+LdfgqAeQV+ZFFerkmz6I2aqTvUoAN4cJSAgFTe5lTweTOQ2vMbGrwf1Jq MXxpvubVlLBRNpeG1niFpb7qfHQ== | |
| Aussteller-Zertifikat | CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, C=AT | |
| Serien-Nr. | 956662 | |
| Dokumentenhinweis | Dieses Dokument wurde amtssigniert. | |