

## **Antwort**

### **der Bundesregierung**

**auf die Kleine Anfrage der Abgeordneten Victor Perli, Dr. Gesine Löttsch, Klaus Ernst, weiterer Abgeordneter und der Fraktion DIE LINKE.**

**– Drucksache 20/8376 –**

### **Prüfung von Kommunikationssoftware durch das Bundesamt für Sicherheit in der Informationstechnik im Allgemeinen und bei Virtual Solution**

#### Vorbemerkung der Fragesteller

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) prüft unter anderem Softwarelösungen für die sichere Kommunikation der Bundesverwaltung. Eine der Firmen, die in der Vergangenheit solche Lösungen bereitgestellt hat, ist Virtual Solution (heute im Eigentum von Materna, siehe [www.spiegel.de/wirtschaft/unternehmen/virtual-solution-umstrittene-it-sicherheitsfirma-verkauft-a-537594af-a2f4-43a7-af4e-71089383f88c](http://www.spiegel.de/wirtschaft/unternehmen/virtual-solution-umstrittene-it-sicherheitsfirma-verkauft-a-537594af-a2f4-43a7-af4e-71089383f88c)).

#### Vorbemerkung der Bundesregierung

Die Bundesregierung geht bei ihrer Antwort davon aus, dass die Begriffe Zertifizierung und Zulassung in dieser Anfrage synonym verwendet werden und dass jeweils Zulassungsverfahren gemäß § 51 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) gemeint sind.

1. Welche Prüfungshandlungen nimmt das Bundesamt für Sicherheit in der Informationstechnik bei initialen Zertifizierungsverfahren für Kommunikationslösungen (Software) vor, die in der Bundesverwaltung eingesetzt wird, etwa zur Sicherung von Kommunikation auf mobilen Geräten?

Alle Prüfungen im Rahmen von Zulassungsverfahren richten sich nach den im Bundesamt für Sicherheit in der Informationstechnik (BSI)-Nachweiskatalog definierten Sicherheitsanforderungen für eine Evaluierung mit dem Ziel der Zulassung für die Verarbeitung von Informationen bis zu einem Geheimhaltungsgrad „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NfD). Diese auch für NATO- und EU-Zulassungen gültigen Kriterien basieren auf den internationalen Standards ISO 15408 (CommonCriteria) und ISO 18045 (Common Methodology for Information Technology Security Evaluation) und definieren einen vollständigen Satz an Anforderungen an die Nachweise für eine Prüfung,

die von Herstellern und Evaluatoren im Rahmen eines VS-NfD Zulassungsverfahrens gemäß VSA erfüllt werden sollen. Ebenfalls enthalten sind Anforderungen zur Prüfung von Produktupdates bei bereits zugelassenen Produkten.

2. Welche Prüfungshandlungen nimmt das BSI bei der Zulassung von Updates bzw. Folgeversionen solcher Kommunikationslösungen bzw. bei der Verlängerung der Zulassung vor?

Trifft es zu, dass über die Zulassung von Upgrades nur nach Aktenlage entschieden wird?

Ebenfalls in den in der Antwort zu Frage 1 genannten Kriterien und Methodik enthalten sind Anforderungen zur Prüfung von Produktupdates bei bereits zugelassenen Produkten.

3. Welche der in den Fragen 1 und 2 genannten Schritte im Zertifizierungsverfahren werden durch externe Dienstleister durchgeführt, und welche weiteren Prüfungsschritte schließen sich im BSI an die Vorlage der Ergebnisse an?

Sämtliche in den Antworten zu den Fragen 1 und 2 genannten Prüfschritte können sowohl durch das BSI als auch durch vom BSI anerkannte Prüfstellen durchgeführt werden. Die Erteilung der Zulassung selbst obliegt auf Grundlage dieser Prüfergebnisse dem im BSI verorteten Zulassungsreferat und richtet sich nach den im BSI verankerten Prozessen des Zulassungsschemas gemäß § 51 Absatz 2 und § 52 Absatz 1, 2 VSA

4. In welchen Fällen in derartigen Zertifizierungsverfahren müssen Anbieter von Kommunikationslösungen dem BSI die Namen von Mitarbeitern bzw. Programmierern mitteilen, die mit der Entwicklung bzw. Weiterentwicklung der Software befasst sind?

Im Rahmen von Zulassungsverfahren wird keine Überprüfung der Mitarbeiter eines Herstellers vorgenommen. Eine formale Grundlage für solche Überprüfungen in Form von Kriterien liegt nicht vor. Ebenfalls liegen dem BSI im Rahmen von Zulassungsverfahren keine Informationen darüber vor, welche spezifischen Mitarbeiter eines Herstellers an der Entwicklung von zuzulassenden Produkten beteiligt sind und welche Arbeiten sie konkret durchführen.

5. Wie überprüft das BSI, dass ausschließlich die gemeldeten Mitarbeiter bzw. Programmierer an der Software arbeiten?
6. Was sind die Konsequenzen, wenn Unternehmen dem BSI unvollständige Namenslisten übermitteln?
7. Was sind die Folgen für eine bereits erteilte Zulassung einer Kommunikationslösung, wenn sich erweist, dass gegenüber dem BSI nichtgemeldete Programmierer an der Weiterentwicklung der Software beteiligt gewesen sind?

Die Fragen 5 bis 7 werden gemeinsam beantwortet.

Wie in der Antwort zu Frage 4 dargestellt, erfolgt keine Erfassung/Überprüfung der konkret an einer Entwicklung beteiligten Mitarbeiter beim Hersteller. Dadurch leiten sich folgerichtig auch keine Konsequenzen und keine Folgen für bereits erteilte Zulassungen ab.

8. Gibt es im initialen Zertifizierungsverfahren für Kommunikationslösungen für die Bundesverwaltung formale Beschränkungen für Mitarbeiter bzw. Programmierer, die an der Software arbeiten (z. B. Ausschluss von Personen, die keine EU-Staatsbürgerschaft haben)?

Es gibt keine formalen Beschränkungen/Kriterien, die Anforderungen oder Einschränkungen zum Einsatz von Mitarbeitern definieren.

9. Dürfen sich an der Weiterentwicklung (Updates) von bereits vom BSI für den Einsatz in der Bundesverwaltung zugelassenen Kommunikationslösungen Personen beteiligen, die keine Staatsbürger eines EU-Staats sind?  
Gibt es Beschränkungen für Staatsbürger bestimmter Nicht-EU-Staaten?
10. Was sind die Folgen für eine bereits durch das BSI erteilte Zulassung einer Kommunikationslösung, wenn sich erweist, dass Nicht-EU-Staatsbürger an der Weiterentwicklung der Software beteiligt gewesen sind?

Die Fragen 9 und 10 werden gemeinsam beantwortet.

Die Antworten zu den Fragen 5 bis 8 beinhalten ebenfalls Weiterentwicklungen von bereits zugelassenen Produkten.

11. Welche Prüfungshandlungen hat das BSI im Rahmen der initialen Zertifizierungsverfahren von Produkten der Firma Virtual Solution (mittlerweile verkauft an Materna) genau vorgenommen?

Die Prüfung und Erteilung der Zulassung erfolgte nach dem in der Antwort zu Frage 1 beschriebenen Verfahren. Darüberhinausgehende Anforderungen an Produkte der Firma Virtual Solution wurden seitens BSI nicht vorgegeben.

12. Wurde bei Updates des Produkts SecurePIM Government SDS bzw. bei der Verlängerung der Zulassung des Produkts die Zulassung ausschließlich auf Grundlage der vom Unternehmen eingereichten Dokumentation erteilt, und wenn ja, ab welcher Version der Software?

Die Prüfung von Produktupdates erfolgte nach den in den Antworten zu den Fragen 1 und 2 beschriebenen Verfahren. Darüberhinausgehende Anforderungen an Produkte der Firma Virtual Solution wurden seitens BSI nicht vorgegeben.

13. Welche Prüfungshandlungen hat das BSI im Rahmen der Freigabe für Produkte der Firma Virtual Solution für den Geheimhaltungsgrad „Verschlussachen – Nur für den Dienstgebrauch“ (VS-NfD) genau vorgenommen?

Auch im Rahmen von Produkt-Freigabeempfehlungen (gemäß § 51 Absatz 5 VSA 2018) entspricht die Vorgehensweise der in Antworten zu den Fragen 1 und 2 beschriebenen Verfahren.

14. In welchen Fällen hat das BSI von der Firma Virtual Solution Listen von Mitarbeitern bzw. Programmierern eingefordert?

Entsprechend der Antwort zu Frage 4 wurde auch von der Firma Virtual Solution keine Liste von Mitarbeitern bzw. Programmierern eingefordert.

15. Wie hat das BSI überprüft, dass ausschließlich die vom Unternehmen benannten Mitarbeiter an der Weiterentwicklung der Software gearbeitet haben?

Entsprechend der Antwort zu Frage 4 wurde auch von der Firma Virtual Solution keine Liste von Mitarbeitern bzw. Programmierern im Rahmen von Produkt-Weiterentwicklungen eingefordert.

16. Ist der Bundesregierung bekannt, ob auch Programmierer aus Nicht-EU-Staaten an der Software von Virtual Solution gearbeitet haben, und wenn ja, aus welchen Staaten kamen diese Programmierer?

Die Mitarbeit von Programmierern aus Nicht-EU-Staaten an einer Software hat keine direkten Auswirkungen auf die in der Antwort zu Frage 1 dargestellte Prüfungshandlung, weshalb derartige Informationen nicht erhoben und vorgehalten werden.

17. Wurde bei der Firma Virtual Solution im Rahmen der Zertifizierungsverfahren geprüft, ob es Diskrepanzen zwischen der Akten- und Dokumentenlage und den programmierten Anwendungen (z. B. Backdoors in Codes o. Ä.) gab?

Die Überprüfung durch das BSI erfolgte nach Maßgabe der in der Antwort zu Frage 1 beschriebenen Verfahrensweise. Zu konkreten produktspezifischen Erkenntnissen äußert sich die Bundesregierung nicht.