Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

GEHEIM
amtlich geheimgehalten

Die VS-Einstufung endet mit
Ablauf des Jahres 2080

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
POSTANSCHRIFT Postfach 1468, 53004 Bonn

TEL +49 (0)228-997799- 5000
FAX +49 (0)228-997799- 5550

E-MAIL referat32@bfdi.bund.de
INTERNET www.datenschutz.bund.de

DATUM Bonn, 25.06.2020
GESCHÄFTSZ. **32-642/054#1001-**

1. Ausfertigung, 11 Seite/n

An den
Präsidenten des Bundeskriminalamts
Herrn Holger Münch - o.V.i.A. -
Thaerstraße 11
65193 Wiesbaden

nachrichtlich:

Bundesministerium des Innern
ÖS I 3
z.Hd. Herrn RD Schollendorf - o.V.i.A. -
Alt-Moabit 140
10557 Berlin

BETREFF **Quellen-TKÜ beim Bundeskriminalamt (BKA)**
HIER Beratungs- und Kontrollbesuch
BEZUG
ANLAGE

Sehr geehrter Herr Präsident,

vom 14.05.2019 bis 15.05.2019 haben meine Mitarbeiter Herr RD Kugelmeier und Herr RD Bergemann einen Beratungs- und Kontrollbesuch beim BKA in [redacted] zur vom BKA selbst entwickelten Software für die sogenannte Quellen-Telekommunikationsüberwachung „Remote Communication Interception Software (RCIS)" [redacted] durchgeführt. Bereits zuvor war vom 29.08.2016 bis 31.08.2016 ein Besuch durchgeführt worden, dessen Erkenntnisse in diesen Bericht einfließen. Die Mitarbeiterinnen und Mitarbeiter der Referate [redacted] und des behördlichen Datenschutzbeauftragten haben das BKA bei dem Besuch vertreten.

GEHEIM
amtlich geheimgehalten

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Haltestelle Husarenstraße

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Für die freundliche Aufnahme meiner Mitarbeiter und die erwiesene Kooperationsbereitschaft während des Besuchs danke ich. Ich bitte nochmals um Verständnis für die späte Absendung des Berichts.

1. Wesentliches Ergebnis:

Die datenschutzrechtliche Kontrolle der Software [redacted] führt zu keiner Beanstandung.

- Die technische Prüfung hat keine Anhaltspunkte dafür ergeben, dass die Software außer der laufenden Telekommunikation weitere Daten erhebt.

- Der Quellcode der Software zur Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) hat sich als gut dokumentiert ergeben und das BKA war in der Lage, den Entwicklungsprozess gut nachvollziehbar darzustellen.

- Anwendungstests haben ergeben, dass die Software bei Beenden der Telekommunikationsverbindung die Überwachung automatisch abbricht. Unter Testbedingungen war diese also weitgehend auf die laufende Telekommunikation beschränkt.

- Ich empfehle, die Software noch besser kontrollierbar zu gestalten. Um dies zu erreichen, sollte der Schwerpunkt stärker darauf gelegt werden, über alle Entwicklungsschritte hinweg nachverfolgbar zu machen, ob die aufgrund rechtlicher Vorgaben formulierten technischen Anforderungen bis in die Ebene des Quellcodes umgesetzt wurden. So könnte beispielsweise der Quellcode innerhalb der Versionsverwaltung zu einzelnen Testcases und dieser wiederum zu den Softwareanforderungen konsequent referenziert werden. Damit würde noch besser nachverfolgbar, ob die Anforderungen sich im Quellcode selbst niederschlagen. Dabei kann auch eine bessere Toolunterstützung durch einen höheren Grad der Automatisierung dienlich sein.

2. Im Einzelnen:

2.1 Sachverhalt

2.1.1 Allgemeine Feststellungen und festgelegter Funktionsumfang RCIS

Gegenstand des Beratungs- und Kontrollbesuchs war die vom BKA selbst entwickelte Software für die Quellen-TKÜ. Gegenstand war die Software [redacted]. Weitere

Versionen der Software - [redacted] sind nicht Gegenstand dieses Berichts und werden in weiteren datenschutzrechtlichen Kontrollen untersucht werden.

Die Software ist geeignet, [redacted]

Die Software ist in der Lage, [redacted].

[redacted]

Die Software ist in ein [redacted]

2.1.2 Quellcode und Dokumentation

Die Anforderungen an die Software hatten BMI und BKA in der Standardisierten Leistungsbeschreibung (SLB) definiert. Zur ersten Version der SLB hatte ich insbesondere mit Schreiben vom 29.08.2012 und vom 03.09.2012 Stellung genommen (V-620/057#0146), zu der aktualisierten Version mit Schreiben vom 15.01.2019.

Das Anforderungsmanagement verwendet als [redacted]. Die Architekturdokumentation und -modellierung erfolgt in dem [redacted]. Der [redacted] verwaltet und [redacted] entwickelt. Die Test- und Releaseumgebungen [redacted].

Die Netzwerke sind [redacted]. Dies hat Auswirkungen auf [redacted]. Zum einen ist [redacted] notwendig. Dies äußert sich etwa darin, dass [redacted] sind. Zum anderen [redacted]. Denn hier ist es [redacted]. Während des Kontrollbesuchs konnte das BKA [redacted].

Ein [redacted]. Die Anforderungen sind [redacted] festgelegt. Dort sind sowohl die gesetzlichen Anforderungen formuliert als auch durch die Anwendungsebene die polizeilich-taktischen Bedürfnisse vorgegeben. Aus der Gesamtheit dieser funktionalen und nicht funktionalen Anforderungen wird ein Architekturmodell erzeugt. Hierzu wird [redacted]. Das Ergebnis [redacted].

Die weitere Nachverfolgung von Anforderungen und Designvorgaben [redacted], welches das BKA [redacted] einsetzt.

2.1.3 Externe Prüfungen

Die neue Software wurde vom BKA selbst vielfach getestet und verschiedenen Prüfungen unterworfen. Als externer Dienstleister hat [redacted]. Die dabei erstellten Unterlagen habe ich ergänzend durchgesehen.

Der Bericht [redacted] bezieht sich auf die Version [redacted].

2.1.4 Testanwendungen

[redacted]

Es wurden mehrere [redacted]. Dabei wurden auch die Netzwerkverbindungen [redacted] getrennt. Beim [redacted] konnte ich mich davon überzeugen, dass die Aufzeichnung der [redacted] unmittelbar beendet wird. Bei [redacted] Trennung der Netzwerkverbindung [redacted] Dies bedeutet, dass [redacted]

Es wurde darüber hinaus eine Fernlöschung der Quellen-TKÜ Software durchgeführt und danach [redacted]. Es erfolgte erwartungsgemäß keine Aufzeichnung [redacted].

[redacted]

2.2 Bewertung

Die datenschutzrechtliche Bewertung beschränkt sich in diesem Bericht auf eine technische Prüfung. [redacted].

Software zur Quellen-TKÜ ist strukturell in grundrechtlicher Hinsicht besonders eingriffsintensiv. Leitgedanke des datenschutzrechtlichen Kontrollbesuchs war deshalb insbesondere die Frage, ob sich die technische Funktionalität von der abstrakten Anforderungsebene bis zur Realisierung transparent nachvollziehen und prüfen lässt.

Ein besonderes Augenmerk war dabei darauf gerichtet, ob die Software über die reine Quellen-TKÜ hinausgehende Funktionalitäten aufweist und die gesetzlich vorge-

schriebenen technischen Sicherungen enthält. Der Nachweis, ob eine Software nicht geforderte bzw. über das Zulässige hinaus gehende Funktionen aufweist, ist allerdings praktisch kaum zu führen. Eine Kontrolle kann insofern immer nur eine Annäherung und Stichprobe sein. Diese wurde vorliegend durch Sichtung der Anforderungs- und Dokumentationslage, durch Sichtung des Berichts [redacted] und durch eine stichprobenartige Einsicht in den Quellcode selbst durchgeführt.

Besondere Herausforderungen sind insbesondere durch die Arbeit in einem größeren Entwicklerteam vorhanden. Dies wird verstärkt durch die gleichzeitig sehr streng auszulegenden Anforderungen. Gleichwohl hat sich insbesondere der Quellcode als gut dokumentiert ergeben und das BKA war in der Lage, den Prozess gut nachvollziehbar darzustellen.

Anwendungstests haben ergeben, dass die Software bei Beenden der Telekommunikationsverbindung die Überwachung automatisch abbricht. Unter Testbedingungen war diese also auf die laufende Telekommunikation beschränkt.

[redacted]

2.2.1 Zulässiger Funktionsumfang und festgelegte Maßstäbe

Der zulässige Funktionsumfang der Software ergibt sich aus § 20l BKAG alt sowie aus dem neugefassten § 100a StPO. Diese Vorschriften werden durch die Standardisierte Leistungsbeschreibung (SLB) konkretisiert.

Für die Quellen-TKÜ ist in Abgrenzung zur sog. Online-Durchsuchung sicherzustellen, die Überwachung auf die laufende Telekommunikation zu beschränken. Der Eingriff in das informationstechnische System muss notwendig sein, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere trotz der Verschlüsselung der Kommunikation zu ermöglichen. Die Anforderungen an die technische Sicherheit sind im Übrigen dieselben, wie im Falle der sog. Online-Durchsuchung.

Für diese bestimmt § 20k BKAG-alt, dass

- an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,
- die technisch vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden,
- eingesetzte Mittel nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme geschützt sind und

- jeder Einsatz des technischen Mittels protokolliert wird.

Diese Vorgaben muss RCIS einhalten. Dies ist durch technische und organisatorische Maßnahmen sicherzustellen. Dies lässt sich nur dann sicher beurteilen, wenn über den gesamten Entwicklungsprozess nachvollziehbare Maßstäbe festgelegt und eingehalten sind.

Auf der ersten Stufe sind die gesetzlichen Vorgaben in der SLB konkretisiert. Eine Ebene tiefer finden sich die weiteren Festschreibungen in den technischen Unterlagen.

2.2.2 Externe Prüfungen

Aus dem Bericht [redacted]

2.2.3 Quellcode und Dokumentation

2.2.3.1 Allgemeine Anmerkungen

Die besondere Herausforderung für das BKA besteht hier darin, den komplexen Entwicklungsprozess auf allen Ebenen korrekt darzustellen und zu dokumentieren. Er betrifft nämlich auf der obersten Ebene die Grundstruktur und Architektur der Software - quasi die „tragenden Bauteile" -, auf einer weiteren Ebene die Hauptfunktionen und schließlich auf den unteren Ebenen untergeordnete Funktionalitäten, aus denen sich die Software im Detail zusammensetzt. Im Ergebnis muss die Software auf allen Ebenen überprüfbar sein. Auch auf den „unteren" Ebenen können die Funktionalitäten die Software und wesentliche Funktionen beeinflussen. Deshalb muss ihre Integration in den Gesamtkontext der Software nachvollziehbar und dokumentiert sein. Softwareentwicklung erfordert also Feedbackschleifen, hinsichtlich der Realisierung des konkreten Softwaredesigns und der Gewährleistung der Funktionalität

von der Entwicklung einzelner Progammteile bzw. Funktionen bis zur Ebene der Architektur und Anforderungen.

[redacted] Die Herausforderung in einer Kontrolle ist insbesondere, eine saubere Verbindung der Dokumentationen einerseits auf der Anforderungs- und Architekturebene und andererseits der Entwicklungsebene sicherzustellen. [redacted]

2.2.3.2. Geprüfte Szenarien

Während des Besuchs haben meine Mitarbeiter Szenarien vorgegeben, mit denen die durchgängig nachvollziehbare Dokumentation geprüft werden sollte. Dazu haben diese auszugsweise einige Funktionalitäten herausgegriffen, um deren Standort sowohl im Quellcode als auch im Anforderungsmanagement nachzuvollziehen. Im Ergebnis hat das BKA die durchgängige Nachvollziehbarkeit darlegen und demonstrieren können.

Diese auszugsweise angesehenen Funktionalitäten waren

- Löschfunktion: Auf welche Weise wird die Software auf dem Zielsystem sauber gelöscht
- Beginn der Telekommunikation [redacted]
- Versendung einer Datei

Die Löschfunktion ist wie oben dargelegt eine der rechtlichen Anforderungen des § 20 BKAG-alt. Diese wird entsprechend in der SLB gefordert. Anhand der Dokumentation des Quellcodes konnte ich die entsprechenden Passagen des Quellcodes zu dieser Funktion identifizieren und ansehen. [redacted]

[redacted] Bei dieser Gelegenheit konnte ich auch Einsicht in weitere Funktionalitäten der Software nehmen, die durch die Löschfunktion „rückgängig" gemacht werden. [redacted] Dabei waren keine Defizite in der Dokumentation des Quellcodes oder unzulässige Funktionalitäten erkennbar. Im Ergebnis konnte ich den Quellcode und seine Dokumentation sowie den Ausführungspfad der Löschfunktion nachvollziehen.

Vereinzelt habe ich anhand stichprobenartiger Code-Bestandteile nach deren Rechtfertigung in den Anforderungen gesucht. Dieses Vorgehen entspricht der umgekehrten Blickrichtung von dem realisierten Code zurück zur Gesamtheit der Anforderungen. Dabei soll nachgewiesen werden, dass nicht mehr und nicht undokumentiert Softwarefunktionalität erstellt wurde als ursprünglich gefordert. [redacted]).

Das zweite Szenario untersuchte, [redacted]. Im Ergebnis konnte ich die Wirkweise der gewählten Softwarelösung sowie die Einhaltung der rechtlichen Rahmenbedingungen nachvollziehen.

Das dritte Szenario behandelte [redacted]

[redacted]. Auch in diesem Szenario war durch Dokumentation und Quellcode die Funktionalität nachvollziehbar.

2.2.4 Testanwendungen

Als weitere Prüfung habe ich [redacted] einen Funktionstest vorgenommen. Der Test ergab keine datenschutzrechtlichen Auffälligkeiten. Insbesondere endete die Überwachung zeitnah mit Wegfall der Netzwerkverbindung. Sowohl die gezeigte Protokollierung wie die Löschung der Software [redacted] verlief entsprechend den datenschutzrechtlichen Anforderungen.

Die TKÜ-Anlage selbst mache ich nicht zum Gegenstand der Kontrolle, die sich insoweit auf die Remote-Software und ihren Einsatz beschränkt. Ich weise in diesem Zusammenhang aber darauf hin, dass aufgezeichnete Gespräche auch teilweise gelöscht werden können müssen, sofern der Schutz des Kernbereichs privater Lebensgestaltung dies erfordert.

2.2.5 Echtbetrieb

[redacted]

Mit freundlichen Grüßen

Ulrich Kelber