Bundeskriminalamt

Der Präsident

POSTANSCHRIFT Bundeskriminalamt · 65173 Wiesbaden

per E-Mail
Innenausschuss

HAUSANSCHRIFT Thaerstraße 11, 65193 Wiesbaden

TEL +49(0)30 5361-26021
FAX +49(0)30 5361-26003
BEARBEITET VON Niemann, Anja
E-MAIL ls4@bka.bund.de
AZ **LS 4 -**
DATUM **19.10.11**

Sehr geehrte Damen und Herren,

im Auftrag von Herrn Ziercke, übersende ich Ihnen seinen Redebeitrag von der heutigen 53. Innenausschusssitzung.

Mit freundlichen Grüßen

gez. Anja Niemann

60 JAHRE 1951 | | | | | | | 2011 BKA

Bundeskriminalamt

Sprechzettel

Anlass:

Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)

TOP	*Sachstandsbericht Quellen-TKÜ*

Erlauben Sie mir, meinem Vortrag ein Fazit voranzustellen:

- Das BKA hat keinen Verfassungsbruch begangen! Das BKA gewährleistet vielmehr eine enge und konsequente, verfassungstreue Umsetzung der Vorgaben des BVerfG zur Online-Durchsuchung und zur Quellen-TKÜ.
- Wir unterscheiden klar zwischen den Funktionalitäten von Online-Durchsuchung und Quellen-TKÜ. Wir missbrauchen diese Funktionalitäten nicht.
- In unsere OLD- und Quellen-TKÜ-Software war zu keinem Zeitpunkt eine rechtswidrige Hintertür zum Aufspielen von Ausspähprogrammen eingebaut. Der jeweilige richterliche Beschluss war der alleinige Maßstab unseres Handelns.
- Wir führen eine systemtechnische Protokollierung aller Zugriffe und Aufspielungen auf den betroffenen Rechner durch. Wir gewährleisten dadurch die Kontrollmöglichkeiten für den Richter wie auch für den Datenschutzbeauftragten.
- Bei der Nutzung von Proxy-Servern im Ausland findet keine Speicherung, sondern lediglich eine Durchleitung von Daten statt.
- Es gibt keinen Zugriff von Dritten auf die Software des BKA. Es gibt auch keinen Missbrauch durch BKA-Beamte, die Beschuldigten belastende Beweise unter-

schieben. Alles dies sind haltlose Verleumdungen und unseriöse Skandalisierungen.

- Die Planung, Durchführung und Nachbereitung von Quellen-TKÜ und Online-Durchsuchung folgen einem detaillierten Phasenkonzept, einschließlich ausdifferenzierter Prüf- und Kontrollmechanismen.

Warum benötigen wir zur Verhinderung von terroristischen Anschlägen und zur Bekämpfung von Organisierter Kriminalität TKÜ, warum Quellen-TKÜ und Online-Durchsuchung?:

- Die Wirksamkeit der TKÜ ist zuletzt im Jahre 2003 vom MPI eindrucksvoll belegt worden: die Anklagequote bei Verfahren, in denen TKÜ eingesetzt wurde, war mit 58 % etwa doppelt so hoch wie im sonstigen Durchschnitt.
- Die Verurteilungsquote lag sogar bei 94 %.
- Daran hat sich nach unserer Einschätzung bis heute nichts geändert. Ca. 70 % der Aufklärungserfolge der OK basieren auf TKÜ-Maßnahmen.

- Im virtuellen Zeitalter stellen wir eine zunehmende Tendenz der Anonymisierung und Kryptierung von Datenspeicherung und Telekommunikation, insbesondere bei der Internettelefonie fest. Wir beobachten, dass sich dies zu einem bedeutsamen Problem einer wirksamen Strafverfolgung entwickelt.
  Hierzu ein Zitat aus der Entscheidung des BVerfG vom 2. 3. 2010, RdNr. 216, zur Vorratsdatenspeicherung:
  - *„Die neuen Telekommunikationsmittel überwinden Zeit und Raum in einer mit anderen Kommunikationsformen unvergleichbaren Weise und grundsätzlich unter Ausschluss der öffentlichen Wahrnehmung.*
  - *Sie erleichtern damit zugleich die verdeckte Kommunikation und Aktion von Straftätern und ermöglichen es auch verstreuten Gruppen von wenigen Personen, sich zusammenzufinden und effektiv zusammenzuarbeiten.*
  - *Durch die praktisch widerstandsfreie Kommunikation wird eine Bündelung von*

Wissen, Handlungsbereitschaft und krimineller Energie möglich, die die Gefahrenabwehr und Strafverfolgung vor neuartige Aufgaben stellt. Manche Straftaten erfolgen unmittelbar mit Hilfe der neuen Technik.

- *Eingebunden in ein Konglomerat von nunmehr technisch miteinander kommunizierenden Rechnern und Rechnernetzen entziehen sich solche Aktivitäten weithin der Beobachtung. Zugleich können sie – etwa durch Angriffe auf die Telekommunikation Dritter – auch neuartige Gefahren darstellen. "*

Zitatende.

Treffender kann man die Veränderungen der Modi Operandi, die Veränderungen der klassischen Tat- und Täterbilder nicht beschreiben.
Es besteht eine Notwendigkeit für die TKÜ auch in der virtuellen Welt, um terroristische Gewalttäter zu detektieren und schwerste Straftaten zu verhindern. Dies ist nicht nur ein Schutzauftrag für die Polizei.

Nun zur Quellen - TKÜ des BKA im Einzelnen:

- Die Quellen-TKÜ grenzt sich von der klassischen TKÜ dadurch ab, dass die Daten nach verdeckter Einbringung einer Überwachungssoftware am Endgerät (der „Quelle") noch vor der Verschlüsselung bzw. nach ihrer Entschlüsselung erhoben werden.
- Bei der Quellen-TKÜ ist der Leistungsumfang der Software beschränkt. Es dürfen nur die Daten im Rahmen eines laufenden Telekommunikationsvorgangs überwacht werden, die für die Versendung in das Kommunikationsnetz vorgesehen sind.
- Durch eine Quellen-TKÜ werden also keine Daten erlangt, die nicht auch durch eine „konventionelle" TKÜ – außer dem Umstand der Kryptierung – erlangt werden können.
- Demgegenüber erfolgt bei der **Online-Durchsuchung** eine gezielte Suche nach auf der Festplatte gespeicherten Daten und deren Ausleitung. Diese ist angesichts der höheren Eingriffstiefe lediglich zur **Abwehr terroristischer Gefahren** zuläs-

sig.

- **<u>Zwischenfazit</u>:** Die Überwachung der Telekommunikation bzw. Maßnahmen der Online-Durchsuchung (OLD) sind kriminalistisch unverzichtbar, wenn das Internet als Tatmittel für schwere und schwerste Kriminalität eingesetzt wird. Es gibt keine vergleichsweise wirksame Alternative, um kryptierte Beweismittel im Internet zu sichern.

  Dabei gilt für den Einsatz von Online-Durchsuchung und Quellen-TKÜ das Ultima Ratio Prinzip.
  Die Quellen-TKÜ kommt nur in Betracht, wenn andere Methoden nicht zum Erfolg führen. Der Zugriff auf den Rechner stellt die Ultima Ratio dar. An der Häufigkeit des Einsatzes zeigt sich das sensible Verständnis der Sicherheitsbehörden mit dem Umgang dieser Instrumente. Auch dies entspricht einer Vorgabe des BVerfG.
- So wurden in der Zuständigkeit des BKA seit Einsatzfähigkeit in 2007/2008 lediglich **23 Quellen-TKÜ-Maßnahmen** durchgeführt:
- Bei **19** Quellen-TKÜ-Maßnahmen handelte es sich um **BKA-eigene Verfahren**, d.h. wir sprechen von durchschnittlich **5 - 6** Maßnahmen pro Jahr!
  - Es handelte sich dabei um **acht** Maßnahmen zur Abwehr terroristischer Gefahren, **elf** Maßnahmen wurden im Rahmen der Strafverfolgung durch Gerichte angeordnet.
- Bei **vier** Maßnahmen war das BKA in **Amtshilfe** zur Unterstützung der Strafverfolgung der Landespolizeien in **Hessen** und **Rheinland-Pfalz** tätig.

- <u>Ein zweites Zwischenfazit:</u> Alle aktuell über die Medien geschürten Horrorszenarien vom Überwachungsstaat und einer außer Rand und Band geratenen Polizei erweisen sich nachweisbar als unseriöse Skandalisierungen. Es gibt weder Millionen, noch Hunderttausende mit Quellen-TKÜ überwachte Rechner, sondern 5 - 6 Maßnahmen durch das BKA pro Jahr – ca. 100 in den letzten Jahren durch alle Si-

cherheitsbehörden zusammen (das sind 16 LKÄ, 16 LfV, BKA, BfV, Zoll, Bundespolizei – also 36 Behörden) in Deutschland.

Lassen Sie mich Ihnen - bevor ich zu den Kritikpunkten des Chaos Computer Clubs Stellung nehme - kurz die **Verfahrensweise zur Quellen-TKÜ und zur OLD im BKA** vorstellen:

- Die Durchführung von QTKÜ erfolgt unter strikter Anwendung eines auch im Rahmen der Zertifizierung nach DIN ISO 9000ff erstellten **Phasenkonzeptes**.
- Das Konzept sieht einen zweistufigen Amtsleitungsvorbehalt und Einhaltung konzeptioneller und technischer Sicherungsmaßnahmen vor.

Das Phasenmodel sieht folgenden chronologischen Ablauf vor:

1. **Beratungsphase (Amtsleitungsvorbehalt!)**
   - geeignetes und zulässiges kriminaltaktisches Mittel
   - rechtlich zulässig
   - verhältnismäßig

2**. Vorbereitungsphase**
   - das Zielsystem wird identifiziert und verifiziert,
   - eine Einbringungsmethode wird identifiziert,
   - das Tool wird abgestimmt und getestet
   - erste Ansätze für Einbringungsmethoden werden erhoben, gesammelt, bewertet
   - die geeignetste Einbringungsmethode wird technisch und inhaltlich intensiv geprüft.

3. **Einbringungsphase (Amtsleitungsvorbehalt bez. auf jede Einbringungsmethode!)**
   - der Beschluss wird zur Durchführung einer Q-TKÜ bei der zuständigen Staatsanwaltschaft angeregt

- mit Vorliegen des richterlichen Beschlusses und der Genehmigung der Amtsleitung BKA wird die Quellen-TKÜ-Software beschafft und auf ihre Funktionen hin ausführlich getestet und überprüft
- Software wird, mit der genehmigten Einbringungsmethode auf den Zielrechner aufgebracht

4. **Durchführungsphase**

- die Erkenntnisse der Q-TKÜ werden inhaltlich und technisch ausgewertet
- Kernbereichsschutz wird im Rahmen der inhaltlichen Auswertung mit Hilfe der Auswertesoftware gewährleistet
- zur Verschleierung der Q-TKÜ gegenüber dem Tatverdächtigen wird die gesamte Kommunikation der Software über mindestens zwei Proxy Server geleitet
- auf diesen Proxy Servern werden keinerlei Daten abgelegt, sondern lediglich eine **Durchleitung** - über nicht-deutsche Server – vorgenommen
- Programmupdates, also Aktualisierungen der überwachten Softwareprodukte werden mithilfe eines beim Hersteller angeforderten Updates behoben
- das Update wird vor dem Einsatz getestet, es ist keine Funktionalität zum unberechtigten Ausspähen von Daten
- Update selbst wird mit der Updatefunktionalität der Digitask-Aufzeichnungseinheit durchgeführt (Updates werden protokolliert)

5. **Beendigungsphase**

- Überwachungssoftware wird möglichst im Rahmen operativer Maßnahmen physikalisch gelöscht
- sofern mangels Zugriff auf das überwachte System physikalisches Löschen nicht realisierbar, wird auf die eingebaute Löschfunktion zurückgegriffen
- bei letztgenannter Alternative (sogen. Fernlöschung) besteht ein Restrisiko, dass die Software oder Teile davon zu einem späteren Zeitpunkt mit forensischen Methoden durch Dritte analysiert werden könnten

6. **Nachbereitungsphase**

- die Nachbereitungsphase dient der Evaluierung und Prozessoptimierung

Protokollierung / Dokumentation

Zur Gewährleistung der Nachvollziehbarkeit der gesamten Q-TKÜ werden verschiedene Dokumentationsschritte vorgenommen und systemtechnische Protokollierungen durchgeführt:

- Die Informationen zu Beschaffung des Tools, Lieferung, Absprachen mit dem Bedarfsträger, Vermerke zu An- und Abschaltung sowie weitere fallrelevante Daten werden archiviert.
- Sämtliche durchgeführten Aktionen (Updates, Modulaktivierungen und -deaktivierungen) werden protokolliert.
- Des Weiteren sind dort alle gewonnenen Daten (Gespräche, Chatnachrichten, übertragene Dateien) auswertbar vorhanden.
- Das systemtechnische Protokoll ist aus der Bedienoberfläche heraus nicht manipulierbar.
- Löschen von Protokolldaten wäre nur mit administrativem Zugang (nicht der Ermittlungsbeamte, nur der Techniker hat Zugang) auf die zugrundeliegende Datenbank und entsprechendem technischen Aufwand bei gleichzeitiger krimineller Energie möglich. Dafür gibt es keinem Fall auch nur die Spur eines Verdachts!
- Die gelieferten Tools werden abgelegt, um deren nachträgliche Prüfung zu ermöglichen.

Zu den Vorwürfen des Chaos Computer Clubs (CCC):

- **Falsch ist,** dass das BKA eine Überwachungssoftware verwendet, die mit einer unsicheren symmetrischen Verschlüsselung arbeitet und nur in eine Kommunikationsrichtung verschlüsselt. Wir verschlüsseln in beide Richtungen!

- **Richtig ist**, dass ein gemeinsamer Schlüssel zwischen Software und Einsatzservern vergeben wird. Dies dient der Verschlüsselung und der Authentifizierung. Der Kommunikationspartner kann sich ohne diesen Schlüssel nicht als gültiger Partner ausgeben. Dritte können nicht widerrechtlich eindringen und durch eine Hintertür evtl. eigene Dateninhalte platzieren.
  Die durch den Chaos Computer Club analysierte Quellen-TKÜ-Software bezieht sich nach Aussage der Herstellerfirma DigiTask und aufgrund der durch den CCC angeführten Produktmerkmale und Programmspezifika auf eine ca. drei Jahre alte Version der Software, die das BKA nicht eingesetzt hat.

  Seit der Veröffentlichung der Signatur der Verschlüsselung durch den CCC-könnten noch laufende Maßnahmen entdeckt werden. Das BKA hat daher in einem aktuellen Verfahren der organisierten Rauschgiftkriminalität die Maßnahme sofort abgebrochen und dies der Staatsanwaltschaft und dem anordnenden Gericht mitgeteilt. Dies ist auch den Bundesländern mitgeteilt worden.
  Die Firma DigiTask hat nach eigener Aussage alle Kunden informiert und ebenfalls empfohlen, laufende Maßnahmen abzubrechen.

- **Es ist falsch**, dass die vom BKA verwendete Q-TKÜ-Software über eine **rechtswidrige** Nachladefunktion verfügt, mit der beliebige Schadmodule nachgeladen werden.

  Die Quellen-TKÜ-Software ist auf das Zielsystem und die dort installierte Skypeversion ausgerichtet. Bei einem Skypeupdate muss daher auch die Quellen-TKÜ-Software angepasst werden, da ansonsten die Kommunikation nicht mehr aufgezeichnet wird. Es kommt durchaus häufig vor, dass die Zielperson eine neue Version von Sykpe auf dem Zielsystem installiert.
  Dies ist kein Verstoß gegen die Verfassung, wie der CCC meint, es ist auch keine Bequemlichkeit der Sicherheitsbehörden, sondern es ist die Gewährleistung der Umsetzung des richterlichen Beschlusses. Anders könnte eine unterbrechungsfreie Überwachungsfunktion nämlich nicht gewährleistet werden. Das BVerfG verbie-

tet in seiner Entscheidung ein Mehr an Funktionalität, wenn – und darauf kommt es dem BVerfG an - die durch eine Nachladefunktion eingesetzte Software zum Ausspähen von weiteren Daten genutzt würde. Das BVerfG hat diese Feststellung in der Abgrenzung von OLD und Quellen-TkÜ getroffen. Gegen eine bloße Aktualisierungsfunktion kann das BVerfG keine Einwände haben, weil sonst die Maßnahme an sich gefährdet wäre. Dass der CCC seine Argumentation in der FAZ vom 18.10.2011 mit dem Beispiel einer Folterandrohung verknüpft, die von Behörden auch als praktisch angesehen werden könnte, disqualifiziert den Autor in bemerkenswerter Weise.

Das BKA hat die Updatefunktion ausschließlich zur Aktualisierung genutzt.

Diese Updatefunktion ist Teil des regulären Funktionsumfangs der Software.

Jede Nutzung der Updatefunktion wird umfassend protokolliert. Darüber hinaus wird ein sog. „Hash“ über das Update gebildet, um eindeutig festzustellen, welches Update wann durchgeführt wurde.

Die Existenz und das Verwenden einer Updatedatenfunktion zur Sicherstellung einer lückenlosen Überwachung der Kommunikation ist von der jeweiligen Befugnisnorm zur Quellen-TKÜ und vom richterlichen Beschluss zur Durchführung der Maßnahme abgedeckt.

Fazit: Diese Updatefunktion gewährleistet die Sicherheit und Funktionalität des Quellen-TKÜ-Tools. Sie stellt sicher, dass die im richterlichen Beschluss verfügten Überwachungsfunktionen unterbrechungsfrei realisiert werden können. Spekulationen über kriminelles Handeln von Behörden, die eine solche Nachladefunktion ermöglichen könnten, entbehrt jeglicher Grundlage. Diese Grundmisstrauen würde letztlich bedeuten, dass jede polizeiliche Maßnahme unter Manipulationsverdacht steht: falsche Observationsberichte, untergeschobene Beweismittel bei Durchsuchungen beschlagnahmte Rauschgiftmengen, die um ein Paar Kilo erhöht werden, unterdrückte Zeugenaussagen usw. usw. Wer dieses Bild der Polizei eines Unrechtsstaates vor Augen hat, lebt mit Sicherheit nicht in Deutschland!

Überprüfung der systemtechnischen Protokollierung im BKA

Wie ich bereits dargestellt habe, beinhaltet das BKA-interne Quellen-TKÜ-Verfahren eine umfassende systemtechnische Protokollierung sämtlicher durchgeführter Aktionen.

- Das BKA hat am 11./12.10.2011 alle Protokolle bisheriger Quellen-TKÜ-Maßnahmen mit der DigiTask-Aufzeichnungseinheit unter Beteiligung der Beauftragten
    - für den Datenschutz sowie
    - für die IT-Sicherheit im BKA

  auf Plausibilität kontrolliert hat.

Im Ergebnis konnten **keine Hinweise** festgestellt werden, dass im BKA eine Software eingesetzt wird, die über die rechtlich zulässigen Grenzen der Quellen-TKÜ hinausgeht und dass im Rahmen der bisher erfolgreich durchgeführten Quellen-TKÜ-Maßnahmen unzulässige Daten ausgeleitet werden.

- **Verschleierung über Proxy-Server in den USA**

- **Falsch ist,** dass mit der Nutzung von ausländischen Proxy-Servern bei der Quellen-TKÜ deutsches Recht umgangen werde. **Richtig ist vielmehr**, das die Daten über einen ausländischen Server lediglich verschlüsselt weitergeleitet und nicht auf dem ausländischen System gespeichert werden. Es handelt sich um das Durchleiten eines verschlüsselten Datenstromes. Damit bleibt deutsches Recht anwendbar und der Rechtsweg zu deutschen Gerichten eröffnet. Es gilt insoweit das Sitzlandprinzip.
- Der Grund für diese Verschleierung ist kriminalistischer Natur. Skype selbst nimmt beim Start automatisch Kontakt mit einem Server in den USA auf. Für den versierten User sollte durch die Quellen-TKÜ- Software kein anderer Eindruck entstehen.

- **Falsch ist die Medienberichterstattung im Spiegel, auf die sich auch der CCC- Autor bezieht,** dass das BKA Einsicht in den Quellcode der Firma Digi-Task hatte.

  Richtig ist, dass der Quellcode der Q-TKÜ-Software der Fa. DigiTask dem BKA nicht offen gelegt wurde. Auch die Quellcodes anderer kommerzieller Anbieter wurden dem BKA nicht offen gelegt.

  Das BKA testet die bestellte Software mit Hilfe eines sogen. Positivtests, der der Funktionalitäten der Software und die Reaktion der vom Zielsystem eingesetzten Sicherheitssoftware (Virenscanner, Firewall) prüft. Die Maßnahme wird als einsatzfähig betrachtet, wenn die bestellten Funktionalitäten vorhanden sind, und die Sicherheitssoftware keine Warnungen produziert. Hierzu werden entsprechend Testdaten generiert (z.B. ein Syketelefonat). Falls ausschließlich ein Loader eingebracht wird, also eine Software, die nur die Updatefunktionalität enthält, werden der erfolgreiche Verbindungsaufbau zur Aufzeichnungseinheit und das Ausbleiben von Warnmeldungen der Sicherheitssoftware geprüft. Durch eine an der Benutzer-Oberfläche der Steuerungssoftware orientierte Funktionsprüfung wird sichergestellt, dass der Funktionsumfang der Software nicht über die im Beschluss zugelassenen und beim Hersteller beantragten Funktionen hinausgeht.

  Alles dies wird umfangreich protokolliert und kann durch den Datenschutzbeauftragten oder den anordnenden Richter kontrolliert werden.

Abschließend möchte ich in Anbetracht teilweise widersprüchlicher Darstellungen in den Medien auf Folgendes hinweisen:

- Die vom BVerfG geforderten rechtlichen Vorgaben sind durch **zwei verschiedene Paragraphen** im BKAG verankert: § 20 k (ODS) und § 20 l (Quellen-TKÜ). Diese enthalten sehr detaillierte Vorgaben für den Einsatz der jeweiligen Software. Ein Blick ins Gesetz lohnt sich!
- Das BKA hat daher die Unterscheidung zwischen Quellen-TKÜ und Online-

Durchsuchung (OLD) auch in technischer Hinsicht immer eingehalten und **verschiedene Software-Tools** eingesetzt. Für die OLD ist eine eigene Software entwickelt worden.

- Der **Kernbereichschutz** wird streng beachtet und intensiv gemeinsam in BKA-Verfahren mit dem zuständigen Richter kontrolliert, der dafür eine mehrseitige Handlungsanleitung selbst erarbeitet hat.
- In der öffentlichen Diskussion um die **strafprozessuale Rechtsgrundlage für die Maßnahme der Quellen-TKÜ** ist bisher fast untergegangen, dass unterschiedliche Rechtsauffassungen im Bundesjustizministerium und den Länderjustizverwaltungen über die Anwendbarkeit von § 100 a ff existieren.
- Diese seit Jahren durch die Justiz nicht geklärte Rechtslage führt zu der absurden Situation, dass der GBA in TE-Verfahren keine Quellen-TKÜ beantragen darf, das BKA aber nach BKAG zur Gefahrenabwehr OLD und Quellen-TKÜ in TE-Lagen durchführt und bei Übernahme der Ermittlungen durch den GBA regelmäßig die Quellen-TKÜ-Maßnahme gefährdet ist, obwohl diese fortgeführt werden müsste. Das wiederum führt dazu, das TE-Verfahren zur Gefahrenabwehr im Einzelfall länger beim BKA bleiben, obwohl der GBA eigentlich übernehmen müsste. Absurd ist auch, dass in den OK-Verfahren der Länderjustizverwaltungen das BKA in Amtshilfe QuellenTKÜ – Maßnhamen durchführt, in den weitaus gefährlicheren TE-Verfahren aber nicht.
- Glauben Sie mir, meine Mitarbeiter verstehen das nicht!