Piratenpartei Sachsen-Anhalt
Postfach 110145
06015 Halle

Landeskriminalamt Sachsen-Anhalt
Direktor Jürgen Schmökel
Lübecker Straße 53-63
39124 Magdeburg

Magdeburg / Halle, 11.10.2011

**“Landestrojaner” Sachsen-Anhalt**

Sehr geehrter Herr Schmökel,

am 08.10.2011 veröffentlichte der Chaos Computer Club (CCC) die Analyse eines ihm in mehrfacher Ausführung zugespielten Schadprogrammes zur Computerspionage. Wie sich im Rahmen der Untersuchung herausstellte, handelte es sich dabei um eine staatliche Software, mit der Ermittlungsbehörden die Computer von Verdächtigen ausspähen können.

In der Analyse wurde weiterhin deutlich, dass der Trojaner unter anderem zusätzliche Schadprogramme nachladen und installieren kann, sowie massive Sicherheitslücken enthält. Für die Überwachung werden zur Verschleierung der Steuerzentrale auch Server in den USA genutzt, wodurch sich weitere Problemfelder in Bezug auf Datenschutz und -sicherheit ergeben. Am schwerwiegendsten jedoch ist die Tatsache, dass die Funktionalität der Software weit über die Grenzen hinaus geht, die das Bundesverfassungsgericht (BVerfG) in seinem Urteil im Jahre 2008 vorgegeben hat.

Mittlerweile haben sich Vermutungen bestätigt, dass mindestens einer der Trojaner aus Bayern stammt und dort bereits mehrfach eingesetzt wurde. Programmiert wurde die Software von der privaten hessischen Firma Digitask. Inzwischen mussten auch das baden-württembergische, das brandenburgische und das niedersächsische Innenministerium die Beschaffung bzw. den Einsatz der Schnüffelsoftware einräumen - das BKA prüft unterdessen weitere Landesbehörden. Das Magdeburger Innenministerium teilte auf Anfrage der Nachrichtenagentur DPA mit: "Die Polizei in Sachsen-Anhalt setzt keine Trojaner zum Ausspähen von mutmaßlichen Straftätern ein. Es habe bislang weder eine Online-Durchsuchung von Computern noch einen Abhörversuch mit spezieller Software auf dem Rechner von Verdächtigen gegeben. Software zur Durchführung dieser Maßnahme ist in Sachsen-Anhalt nicht vorhanden.»

Unter dem Aktenzeichen 13.25-81261-511/11 findet man jedoch im Internet Daten über einen vergebenen Auftrag des Technischen Polizeiamtes Sachsen-Anhalt vom 29.04.2011 (siehe Anlage). nter der vielsagenden Auftragsbezeichnung "Archivierungssystem für Telekommunikationssystem" wurde hier ein Auftrag ausgerechnet an die hessische Firma Digitask vergeben, die auch Lieferant des sogenannten Bayerntrojaners war. Der Verdacht liegt also nahe dass es sich beim genannten Auftrag um einen Vorgang in Zusammenhang mit eben jener Software handelt und der sogenannte "Staatstrojaner" somit entgegen der Aussage des Innenministeriums doch in Sachsen-Anhalt existiert bzw. eingesetzt wird.

Zur Aufklärung des Sachverhaltes stellen wir Ihnen bzw. Ihrer Behörde folgende Fragen und bitten um zeitnahe Beantwortung:

- 1. Wurde oder wird die durch den CCC analysierte Software – oder Software mit vergleichbarer Funktionalität – auch durch das Landeskriminalamt Sachsen-Anhalt oder andere Behörden des Landes Sachsen-Anhalt genutzt? Wann wurde die Software beauftragt, wann abgenommen, seit wann ist sie im Einsatz?
- 2. In wie vielen und welchen Fällen wurde oder wird dieser „Staatstrojaner“ oder Software mit vergleichbarer Funktionalität im Land Sachsen-Anhalt bereits eingesetzt?
- 3. In welchen Fällen ist der Einsatz der vom CCC analysierten Software Ihrer Ansicht nach angemessen und gerechtfertigt und in welchen nicht?
- 4. Auf welchen Rechtsgrundlagen beruhte und beruht der Einsatz im Land Sachsen-Anhalt?
- 5. Wie wurde und wird solche Software auf Gesetzeskonformität überprüft?
- 6. Welchen Umfang an Überwachungsmaßnahmen und welche weiteren Möglichkeiten bietet die Software?
- 7. Welche Behörde hat Entwicklung, Kauf oder Lizenzierung der Software in Auftrag gegeben? Wer war für die Beauftragung und die Abnahme der Software verantwortlich? Welche Personen in der Landesregierung waren darüber informiert? Erfolgte die Softwareentwicklung intern oder wurde damit eine externe Firma beauftragt? Wenn letzteres zutrifft, um welche Firma handelt es sich? Wurde die Verwaltung, Betreuung oder Datensammlung einer privaten Firma übertragen?
- 8. Für wen arbeitete die beauftragte Firma zusätzlich? Waren anderen Behörden des Landes Sachsen-Anhalt oder Behörden anderer Länder die grundsätzlichen Defizite der Software bekannt?
- 9. Wie wurde, im Falle einer externen Beauftragung zur Programmierung der Software, sichergestellt, dass die beauftragte Firma entsprechend zertifiziert ist, solche Aufträge zu bearbeiten? Führte die externe Firma ein Sicherheitsaudit der Software durch, beziehungsweise wurde dieses Audit von einem unabhängigen Unternehmen oder einer anderen Institution, wie zum Beispiel dem BSI, durchgeführt? Wenn nein, wieso nicht?
- 10. Sind weitere Versionen der Software in Entwicklung und wenn ja, welche neuen Eigenschaften sollen diese Versionen bekommen?
- 11. Sind weitere Softwaremodule zur dynamischen Erweiterung des Trojaners mit dem eigentlichen Grundprogramm mitgeliefert worden, die dem Verfassungsgerichtsurteil vom 27.2.2008 widersprechen (BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz Nr. 3-4)?
- 12. War den beauftragenden Behörden vor dem ersten Einsatz der Software bekannt, dass der Zugriff auf die Software ohne Authentifizierung stattfindet und auch von nicht dazu autorisierten Personen beliebige, weitere Software zur Ausführung gebracht werden kann? Wurden diese Funktionen konkret beauftragt oder hat die beauftragte Firma die Software ohne expliziten Auftrag mit diesen Sicherheitslücken ausgestattet?
- 13. Gibt es besondere Handlungsanweisungen zur Wahrung der Rechte der ausgespähten Personen und anderer Unbeteiligter? Wenn ja, wie lauten diese?
- 14. Von wem wird beziehungsweise wurde die Software installiert und ausgeführt? Auf welchen Wegen gelangt sie auf das Endgerät des zu Überwachenden und in welcher Weise wird das Endgerät des zu Überwachenden manipuliert? Sind Hardwareeingriffe notwendig, um die Überwachung durchzuführen?

- 15. Hat es Absprachen mit Internetdienstanbietern gegeben, um deren Infrastruktur und/oder Hard- und Software zur mittelbaren oder unmittelbaren Infektion des Zielrechners einzusetzen? Wenn ja, welche Firmen waren hier involviert?
- 16. Auf welche Weise setzt sich die Software im System fest und welche Dateien sind davon betroffen?
- 17. Sind Hersteller von Geräten und Programmen zur Sicherheit von Computern und Netzwerken (zum Beispiel Firewalls und Antivirenprogramme) mit eingebunden, so dass die Software und die verwendeten Methoden bewusst nicht von diesen Schutzprogrammen erkannt wird? Wurde anderweitig dafür gesorgt, dass Programme zum Aufspüren von Trojanern die Software nicht erkennen konnten?
- 18. Inwieweit kann die eingesetzte Software gängige Anonymisierungs- und Verschlüsselungsmechanismen wie zum Beispiel TLS, AES, Onion Routing umgehen beziehungsweise manipulieren?
- 19. Welchem Stand der Technik entspricht die Software? Wie viel Zeit ist zwischen der Planung und Auftragsvergabe bis hin zur Auslieferung und dem ersten Einsatz der Software vergangen? Wurden die Software-Lizenzen (zum Beispiel für den Speex-Codec) konsequent eingehalten?
- 20. Über welchen Weg gelangen die Daten vom überwachten Endgerät zu den Ermittlungsbehörden?
- 21. Durch welche Netzwerke werden die Daten ausgespähter Personen geleitet? Welche Firmen, Behörden und/oder andere, dritte Personen und Institutionen haben Zugriff auf die benötigten Server, zum Beispiel auf einen Command-and-Control-Server?
- 22. In welchem Maße wurden beziehungsweise werden die so gewonnenen Erkenntnisse verwertet?
- 23. Durch welche Maßnahmen wurde und wird eine Manipulation der Ermittlungen durch Dritte verhindert bzw. erschwert? Wie wurde und wird eine Manipulation der Daten auf diesem Weg ausgeschlossen?
- 24. Wie wurde und wird sichergestellt, dass der Überwachte nach der Entdeckung der Software diese oder deren gesammelten Ergebnisse vor der Übersendung an die einschlägigen Server nicht manipulieren oder entfernen kann?
- 25. Inwieweit ist die Software selbstständig in der Lage, sich innerhalb eines Computernetzwerkes zu verbreiten, um so Zweit- oder Drittgeräte des Überwachten oder anderer, auch unbeteiligter Dritter, zu infiltrieren?
- 26. Steht die Software für unterschiedliche Betriebssystem-Plattformen zur Verfügung oder könnten sich Zielpersonen durch Verwendung von alternativen Betriebssystemen der Überwachung entziehen? Falls ja, um welche Betriebssysteme handelt es sich?
- 27. Wie wird sichergestellt, dass der Überwachte nach der Überwachungsaktion über den Vorgang informiert wird? Ist dies in allen bisherigen Maßnahmen erfolgt? Wenn nein, aus welchen Gründen ist dies nicht erfolgt?
- 28. Ist es möglich sicherzustellen, dass keine Programme oder Dateien auf das System des Überwachten übertragen und/oder ausgeführt wurden? Wenn ja, wie wird dies beweissicher festgestellt?
- 29. Welche konkreten Maßnahmen werden getroffen, um zu verhindern, dass einzelne Beamte missbräuchlich an persönliche Daten gelangen, die gesondert durch das Grundgesetz und besonders durch das Urteil des BVerfG im Jahr 2008 geschützt sind? ("Grundrecht auf

Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme")

- 30. Inwieweit kann ausgeschlossen werden, dass Informationen und Daten des unantastbaren Kernbereiches privater Lebensgestaltung nicht erfasst werden?
- 31. Kann es ausgeschlossen werden, dass derartige Daten den Hoheitsbereich der deutschen Strafverfolgung verlassen? Befindet sich ein Teil der eingesetzten Netzwerk-Infrastruktur im Ausland? Wenn ja, wieso und auf welcher rechtlichen Grundlage? Wem gehören im Ausland genutzte Server? Wer hat Zugriff auf im Ausland genutzte Server?
- 32. In welcher Form und wie lange werden die ermittelten Daten sowie deren Auswertung gespeichert? Stehen diese Daten auch anderen Behörden zur Verfügung?
- 33. Wie wurde und wird der Schutz Dritter gewährleistet, die zufällig in Kontakt mit einer Zielperson stehen, aber im ermittelten Fall nicht betroffen sind?
- 34. Wie wird sichergestellt, dass es sich bei dem überwachten Rechner um den Rechner der Zielperson handelt, beziehungsweise er allein von dieser Person benutzt wurde und die gewonnen Erkenntnisse zweifelsfrei und eindeutig diesem Benutzer zugeordnet werden können?
- 35. Ist es beabsichtigt – in Anbetracht der Manipulationsmöglichkeit und Anfälligkeit der Beweismittelsicherung durch die Software – betroffene Ermittlungsverfahren erneut aufzunehmen, da die Beweissicherheit nicht gewährleistet werden kann?
- 36. Welche Kosten sind durch die Entwicklung, welche beim Einsatz der Software entstanden und werden voraussichtlich noch entstehen? Von wem werden diese Kosten getragen?
- 37. Wie ist die Gewährleistung für die Software vertraglich geregelt? Welche Fristen haben etwaige Wartungsverträge?
- 38. Wer im Land Sachsen-Anhalt ist bei Einsätzen der Software im Einzelfall in der Verantwortung gewesen und hat deren Einsatz autorisiert?
- 39. Welche Landes- sowie Bundesbehörden sind zwecks Amtshilfe an dem jeweiligen Einsatz der Software beteiligt gewesen?
- 40. In welcher Form erfolgt die Archivierung der gesammelten Daten? Wie ist sichergestellt, dass keine Unbefugten Zugriff auf diese Daten bekommen?

Wir weisen Sie darauf hin, dass wir diesen Brief auf der Webseite unseres Landesverbandes veröffentlichen werden, ebenso Ihre Antwort. Wir gehen davon aus, dass Sie uns alle Fragen vollständig und umfassend beantworten werden und bedanken uns bereits im Voraus für Ihr Bemühen.

Mit freundlichen Grüßen

Hennig Lübbers

- Vorstandsvorsitzender -
in Vertretung und im Auftrag des Landesverbandes
Sachsen-Anhalt der Piratenpartei Deutschland

Archivierungssystem für Telekommunikationssystem.



# Archivierungssystem für Telekommunikationssystem.



## BEKANNTMACHUNG ÜBER VERGEBENE AUFTRÄGE

### Lieferauftrag

ABSCHNITT I: ÖFFENTLICHER AUFTRAGGEBER

I.1)**NAME, ADRESSEN UND KONTAKTSTELLE(N)**
Technisches Polizeiamt Sachsen-Anhalt
August-Bebel-Damm 19
z. H. Frau Herrmann
39126 Magdeburg
DEUTSCHLAND
Tel. +49 3915075-611
E-Mail:
Fax +49 3915075-105

**Internet-Adresse(n)**

Hauptadresse des Auftraggebers www.polizei.sachsen-anhalt.de

I.2)**ART DES ÖFFENTLICHEN AUFTRAGGEBERS UND HAUPTTÄTIGKEIT(EN)**
Einrichtung des öffentlichen Rechts
Öffentliche Sicherheit und Ordnung
Der öffentliche Auftraggeber beschafft im Auftrag anderer öffentlicher Auftraggeber Nein
ABSCHNITT II: AUFTRAGSGEGENSTAND

II.1)**BESCHREIBUNG**
II.1.1)**Bezeichnung des Auftrags durch den Auftraggeber**
Archivierungssystem für Telekommunikationssystem.
II.1.2)**Art des Auftrags und Ort der Ausführung, der Lieferung bzw. der Dienstleistung**
Lieferauftrag
Kauf
Hauptlieferort Magdeburg.
NUTS-Code DEE03

II.1.3)**Gegenstand der Bekanntmachung**
II.1.4)**Kurze Beschreibung des Auftrags oder Beschaffungsvorhabens**
Archivierungssystem für Telekommunikationssystem.
II.1.5)**Gemeinsames Vokabular für öffentliche Aufträge (CPV)**
30234000

II.1.6)**Auftrag fällt unter das Beschaffungsübereinkommen (GPA)**
Ja
II.2)**ENDGÜLTIGER GESAMTWERT DES AUFTRAGS**
II.2.1)**Endgültiger Gesamtwert des Auftrags**
ABSCHNITT IV: VERFAHREN

IV.1)**VERFAHRENSART**
IV.1.1)**Verfahrensart**
Verhandlungsverfahren ohne Aufruf zum Wettbewerb
Begründung für die Auftragsvergabe ohne vorherige Veröffentlichung einer Vergabebekanntmachung im Amtsblatt der Europäischen Union:
c) Die Bauleistungen/Lieferungen/Dienstleistungen können nur von einem bestimmten Bieter ausgeführt werden, und zwar aus technischen Gründen
IV.2)**ZUSCHLAGSKRITERIEN**
IV.2.1)**Zuschlagskriterien**
IV.2.2)**Es wurde eine elektronische Auktion durchgeführt**
Nein
IV.3)**VERWALTUNGSINFORMATIONEN**
IV.3.1)**Aktenzeichen beim öffentlichen Auftraggeber**
13.25-81261-511/11
IV.3.2)**Frühere Bekanntmachungen desselben Auftrags**
Nein
ABSCHNITT V: AUFTRAGSVERGABE

AUFTRAGS-NR.: 13.25-81261-511/11BEZEICHNUNG Archivierungssystem.
V.1)**Tag der Auftragsvergabe**
14.4.2011
V.2)**ZAHL DER EINGEGANGENEN ANGEBOTE:**
1
V.3)**Name und Anschrift des Wirtschaftsteilnehmers, an den der Auftrag vergeben wurde**

**Wähle ein Land**

Baden-Württemberg
Bayern
Berlin
Brandenburg
Bremen
Hamburg
Hessen
Mecklenburg-Vorpommern
Niedersachsen
Nordrhein-Westfalen
Rheinland-Pfalz
Saarland
Sachsen
**Sachsen-Anhalt**
Schleswig-Holstein
Thüringen

**Wähle einen Ort aus Sachsen-Anhalt**

Gardelegen
Arendsee
Aschersleben
Bernburg (Saale)
Bitterfeld-Wolfen
Burg
Dessau-Roßlau
Dingelstedt am Huy
Dolle
Droyßig
Gatersleben
Genthin
Goldbeck
Halberstadt
Haldensleben
Halle(Saale)
Hansestadt Seehausen (Altmark)
Hecklingen
Hettstedt
Heyrothsberge
Hohe Börde
Ilsenburg
Jerichow
Kalbe
Kemberg
Klötze
Köthen (Anhalt)
Leuna
Lutherstadt Eisleben
Lutherstadt Wittenberg

DigiTask GmbH
Hüttenstr. 58
35708 Haiger
DEUTSCHLAND

V.4)**ANGABEN ZUM AUFTRAGSWERT**
V.5)**ES KÖNNEN UNTERAUFTRÄGE/SUBAUFTRÄGE VERGEBEN WERDEN**
Nein
ABSCHNITT VI: ZUSÄTZLICHE INFORMATIONEN

VI.1)**AUFTRAG IN VERBINDUNG MIT EINEM VORHABEN UND/ODER PROGRAMM, DAS AUS GEMEINSCHAFTSMITTELN FINANZIERT WIRD**
Nein
VI.2)**SONSTIGE INFORMATIONEN**
VI.3)**RECHTSBEHELFSVERFAHREN/NACHPRÜFUNGSVERFAHREN**
VI.3.1)**Zuständige Stelle für Nachprüfungsverfahren**
2. Vergabekammer beim Landesverwaltungsamt
Ernst-Kamieth-Str. 2
06112 Halle
DEUTSCHLAND
E-Mail:
Tel. +49 3455141536
Internet: www.sachsen-anhalt.de
Fax +49 3455141115

VI.3.2)**Einlegung von Rechtsbehelfen**
Genaue Angaben zu den Fristen für die Einlegung von Rechtsbehelfen: Frist für Nachprüfungsverfahren nach § 107 Gesetz gegen Wettbewerbsbeschränkungen (GWB): Gemäß § 107 Abs. 3 Nr. 4 GWB ist der Antrag zum Nachprüfungsverfahren unzulässig, soweit mehr als 15 Kalendertage nach Eingang der Mitteilung des Auftraggebers, einer Rüge nicht abhelfen zu wollen, vergangen sind.
VI.3.3)**Stelle, bei der Auskünfte über die Einlegung von Rechtsbehelfen erhältlich sind**
VI.4)**TAG DER ABSENDUNG DIESER BEKANNTMACHUNG:**
21.4.2011

**Magdeburg**
Merseburg
Mieste
Mücheln
Naumburg
Niedere Börde
Oschersleben
Osterburg
Quedlinburg
Salzwedel
Sandersdorf-Brehna
Sangerhausen
Schkopau
Schönebeck (Elbe)
Staßfurt
Stendal
Sülzetal
Tangermünde
Thale
Uchtspringe
Wanzleben-Börde
Weißenfels
Wernigerode
Zahna-Elster
Zeitz
Zerbst