Bundesnetzagentur

Fragenkatalog zur Anhörung der Unternehmen am Fr., 09.08.2013

1. Sind Sie gegenüber einer amerikanischen oder britischen Stelle zur Geheimhaltung über eine Zusammenarbeit verpflichtet?

   - Worauf bezieht sich diese Pflicht und wem gegenüber besteht sie?
   - Sind Sie in der Lage, die Frage nach der Zusammenarbeit wahrheitsgemäß zu beantworten?

2. Welche Form der Zusammenarbeit gibt es?

3. Aussage: „Faktisch habe der GCHQ (UK Government Communications Headquarters) einen Teil seiner Ausspäharbeit an Privatunternehmen delegiert!"
Wie ist hier der Sachstand?

5. Auf welchen Rechtsgrundlagen bzw Vertragsgrundlagen basiert die Zusammenarbeit nach Punkt 1 – 3.

6. Können Sie mit den öffentlich bekannt gewordenen Bezeichnungen / Decknamen / Codename etwas anfangen?
Verizon Business, Codename: "Dacron",
British Telecommunications ("Remedy"),
Vodafone Cable ("Gerontic"),
Global Crossing ("Pinnage"),
Level 3 ("Little"),
Viatel ("Vitreous") und
Interoute ("Streetcar").

7. Was sagt Ihnen die Bezeichnung "Mastering the Internet"? (Ein Programm der GCHQ)

8. Stimmt die Aussage „Jede der sieben Firmen ist demnach für das Abhören eines eigenen Teils des weltweiten Glasfasernetzes verantwortlich."?

9. Verizon (zitiert nach SZ vom 02.08.13): „"Die Gesetze eines jeden Landes, auch in Großbritannien und Deutschland, erlauben den Regierungen, ein Unternehmen unter bestimmten Umständen zur Herausgabe von Informationen zu verpflichten."
Verallgemeinert: Wurden Sie durch Gesetze Ihres Landes verpflichtet, „Daten auf deutschem Boden" abzugreifen? (Welche Gesetze welches Landes ?)

10. Welche Rolle spielt hierbei der *Foreign Intelligence Surveillance Court*?

(Bereits Anfang Juni war von der SZ behauptet worden, dass Verizon vom amerikanischen Geheimgericht Foreign Intelligence Surveillance Court gezwungen wurde, dem US-Geheimdienst National Security Agency "eine elektronische Kopie" sämtlicher Verbindungsdaten zu übergeben)

11. Haben Sie eine Vermutung, warum ausgerechnet ihr Unternehmen in den „Enthüllungen" genannt wurde?

12. Haben Sie Indizien dafür, dass auch Daten (Bestands- Verkehrs- oder Inhaltsdaten)aus Ihrem Geschäftsbereich ausgespäht wurden?

Bundesnetzagentur

13. Liegen Anhaltspunkte dafür vor, dass z.B. Trojanersoftware in Ihren Anlagen installiert wurde.

14. Betreibt Ihr Unternehmen Überwachungseinrichtungen nach § 110 Abs. 1 TKG zur Umsetzung von Überwachungsmaßnahmen der Individualkommunikation und/oder zur Beauskunftung von Bestands- und/oder Verkehrsdaten?

15. Betreibt Ihr Unternahmen Überwachungseinrichtungen nach den §§ 26-29 TKÜV zur Umsetzung sogenannter strategischer Beschränkungen nach den §§ 5 und 8 G10-Gesetz?

16. Wenn derartige Anlagen betrieben werden, werden hierfür auch die Regelungen zur Protokollierung der Nutzungen dieser Einrichtungen sowie der Kontrolle dieser Protokollierungen eingehalten?

17. Gab oder gibt es besondere Vorkommnisse, die im Rahmen der Protokollprüfung oder sonstiger Prüfungen der Überwachungseinrichtungen aufgefallen sind, die über eine vereinzelte Fehlbedienung hinausgeht?

18. Wird die Vorgabe zum beschränkten Zugang zu diesen Systemen eingehalten?

19. Werden darüber hinaus Systeme unterhalten, die eine Erstellung einer Kopie der Telekommunikation ermöglichen und wenn ja, wie wird deren Einsatz kontrolliert?

20. Falls Daten aus Ihrem Geschäftsbereich tangiert waren, haben Sie geprüft, ob die im Zusammenhang mit Ihrem Sicherheitskonzept erstellte Gefährdungsanalyse noch den aktuellen Gegebenheiten entspricht?

21. Haben Sie überprüft, ob die von Ihnen getroffenen technischen oder organisatorischen Schutzmaßnahmen gemäß § 109 Abs. 1 und 2 TKG ausreichend sind?

22. Ist die Überarbeitung Ihres Sicherheitskonzeptes (aus gegebenem Anlass) vorgesehen?

Anmerkung:

Je nach Ergebnissen der Ermittlungen wird die BNetzA auch den Katalog von Sicherheitsanforderungen aktualisieren.