BILD: Deutschland ist jetzt zum wiederholten Male Ziel eines massiven Hacker-Angriffs geworden. Ist das nur ein Vorgeschmack auf das was noch kommt, Herr Bundesinnenminister?

Thomas de Maizière: „Wir leben in einer digitalen Welt und natürlich sind wir hier genauso angreifbar wie im anderen Leben auch. Das wissen wir auch nicht erst seit den Angriffen vom Sonntag. Ich habe 2015 ein IT-Sicherheitsgesetz vorgelegt und in den vergangenen Jahren kontinuierlich das BSI finanziell und personell ausgebaut. Wir befinden uns mit den Angreifern im ständigen Wettstreit. Mit der im November im Kabinett verabschiedeten Cybersicherheitsstrategie haben wir weitere Maßnahmen zum Schutz unserer Informationsinfrastrukturen festgelegt. Dennoch werden wir immer wieder einzelne Vorfälle erleben. Gemeinsam werden Staat und Wirtschaft hier ihre Anstrengungen noch einmal verstärken müssen."

BILD: Wer steckt hinter dem Angriff auf die Deutsche Telekom AG?

De Maizière: „Bei dem jetzigen Angriff handelt es sich nach den uns vorliegenden Erkenntnissen um einen Angriff durch das sogenannte Mirai-Botnetz. Durch eine Angriffssoftware wird versucht, die Kontrolle von Geräten im Netz - hier waren es Internet-Router - zu übernehmen, also zu kapern. Derartig kontrollierte Geräte („Bots") können dazu genutzt werden, Webseiten im Netz durch immense Datenmengen zu überfluten und dadurch für Dritte nicht mehr erreichbar zu machen."

BILD: Vor kurzem haben Sie vor Hacker-Angriffen der Russen während des Bundestagswahlkampfs 2017 gewarnt. Heute hat sich Ihnen der BND-Präsident angeschlossen. Wie ernst ist die Cyber-Bedrohung aus Russland und übt Putin schon für die Wahl?

De Maizière: „Wir müssen unterscheiden, ob es sich bei Angreifern im Cyberraum um staatliche Stellen oder Kriminelle handelt. Diese Feststellung ist aber nicht immer einfach zu treffen. Umso mehr gilt, dass wir unsere Infrastrukturen mit äußerster Sorgfalt schützen und eventuellen Einflussnahmen massiv entgegentreten werden. Etwas anderes sind Verfälschungen. Wir müssen aufklären, inwieweit soziale

Medien durch Falschmeldungen für manipulierende Meinungsbildung missbraucht werden können. Wir wollen, dass hinter jeder Meinung ein Mensch steht und keine Maschine."

BILD: Wie löchrig ist deutsche Cyber-Abwehr?

De Maizière: „Mit der Gründung des Nationalen Cyber-Abwehrzentrum in 2011 haben wir ein geeignetes Instrument, um - wie Sie sagen würden - unsere „Löcher" in der Cyberabwehr zu schließen. Auch der Cybersicherheitsrat, in dem die Wirtschaft und die Bundesländer mitarbeiten, leistet einen wichtigen Beitrag, die erforderlichen Maßnahmen zwischen allen Verantwortlichen abzustimmen. Jetzt entwickeln wir insbesondere das Cyber-Abwehrzentrum weiter wir müssen operativ noch besser werden, da sind wir dran. Auch das IT-Sicherheitsgesetz aus dem letzten Jahr versetzt uns in die Lage, unsere Kritischen Infrastrukturen besser zu schützen.

BILD: Können Sie Deutschland und seine Bürger vor der Bedrohung aus dem Netz überhaupt wirksam schützen?

De Maizière: „Wir machen hier bereits sehr viel. Das fängt mit einer angemessenen Aufklärung an. Hier unterstützt uns etwa der Verein „Deutschland sicher im Netz e.V.". Auch die Vorgaben für Diensteanbieter im Netz wurden durch das IT-Sicherheitsgesetz angehoben. Außerdem verfügen wir in Deutschland über eine starke IT-Sicherheitsindustrie, die gute Produkte bereitstellt. Allerdings müssen die Bürgerinnen und Bürger die Angebote auch nutzen. Das Zauberwort ist Sensibilisierung. Den Sicherheitsgurt muss ich auch anlegen, sonst schützt er mich nicht. Ich habe mich vor allem auch für Deutschland als Verschlüsselungsstandort Nr. 1 eingesetzt. Jeder kann seine private Kommunikation und seine Daten durch starke Verschlüsselungsprogramme schützen. Auch Firewalls und Anti-Viren-Software leisten gute Dienste. Es ist aber wie sonst auch: wir können alle nur das Mögliche machen, das aber machen wir.

BILD: 900.000 Telekom-Kunden waren ohne eigene Schuld von dem Hacker-Angriff betroffen. Ist das ein Versagen der Deutschen Telekom?

De Maizière: „Das kann nur das Unternehmen beantworten. Die Zusammenarbeit mit dem BSI war und ist gut."

BILD: Brauchen wir eine Haftungspflicht für Firmen, die IT-Geräte herstellen?

De Maizière: „ Ja, ‚mehr Haftung als bisher. Im Internet wollen sich alle frei bewegen, aber keiner für irgendetwas haften. Das geht nicht. Verantwortung für die digitale Sicherheit tragen Nutzer, Management in Unternehmen und Behörden, Hersteller, Provider und Dienstanbieter gleichermaßen. Dabei geht es um eine faire Lastenverteilung. Dies scheint mir im Bereich der Endprodukte beim Anwender nicht immer gegeben. Verbraucher müssen jedenfalls auf die Sicherheit der auf dem Markt befindlichen IT-Produkte vertrauen können."

## Pletat, Heiko

| | |
|---|---|
| **Von:** | Reisen, Andreas |
| **Gesendet:** | Donnerstag, 8. Dezember 2016 13:51 |
| **An:** | Gobel, Kathleen |
| **Cc:** | Pletat, Heiko; Fischer, Matthias |
| **Betreff:** | WG: Vorbereitung IA zu Telekom Vorfall |
| **Anlagen:** | 161208 Vorbereitung 99.IA zu Telekom Vorfall.docx |

zK

---

**Von:** Reisen, Andreas
**Gesendet:** Donnerstag, 8. Dezember 2016 13:51
**An:** OeSII4_; ITII1_; ITII3_; ITII4_
**Betreff:** Vorbereitung IA zu Telekom Vorfall

Liebe Kolleginnen und Kollegen,

ich bitte um Mitzeichnung bis heute 15:30 Uhr.

Für die kurze Fristsetzung bitte ich um Nachsicht. Die Vorlage an KabParl muss noch heute erfolgen.

Mit freundlichen Grüßen, Andreas Reisen

**Referat IT II 2**
ITII2-12003/3#4
RefL.: MinR Reisen
Sb.: RAFr Gobel

Berlin, den 08.12.2016
Hausruf: -11993

**Sitzung des Innen-Ausschusses des Deutschen Bundestages**
am 14. Dezember 2016
Punkt 1a der Tagesordnung

Betreff: Bericht der BReg zu Erkenntnissen über den Cyberangriff gegen Systeme der Deutschen Telekom AG

Anlage: Cyber-Lage vom 29.11.16 und 01.12.16

über

Herrn L Stab ITII Herrn Abteilungsleiter IT

dem Referat Kabinett- und Parlamentsangelegenheiten zur weiteren Veranlassung vorgelegt.

**1. Votum und Kurzerläuterung**

☐ Zustimmung ☐ Ablehnung ☒ Kenntnisnahme

**2. Teilnehmer (BMI/andere Ressorts) an der Ausschusssitzung**

LStab IT II / ÖS III
P BSI
Herr Dr. Häger (BSI)
(Herr Dr. Kremer (Vorstandsmitglied Dt. Telekom)
Herr Tschersich (Leiter Group Security Dt. Telekom))

## 3. Sachverhalt

Beschreibung des Vorfalls:

Am 27. und 28. November 2016 waren ca. 950.000 Kundenanschlüsse der Deutschen Telekom AG (DTAG) von Internet- und Telefonieausfällen betroffen. Dabei handelte es sich um einen weltweiten ungezielten Angriff durch Mirai-Botnet-Schad-Software, um Router zu infizieren und zu einem erweiterten Botnetz zusammenzuschließen. Diese Angriffsversuche galten nicht speziell der DTAG oder deren Kunden. Auch das Regierungsnetz wurde attackiert, aber wegen der vorhandenen Sicherheitsinfrastruktur und zusätzlichen Filtermaßnahmen des BSI nicht kompromittiert.

Nach bisherigen Erkenntnissen waren in D nur Endkundengeräte (Router) der Telekom des Herstellers Arcadyan betroffen. Der Angriff führte nicht zu einer Infektion und damit zu einer möglichen Fernsteuerung der Router sondern „nur" zu einem Geräteabsturz. Die Telekom konnte innerhalb von ca. 12 Stunden die Systemintegrität bei ihren Kunden wiederherstellen. Nach unbestätigten Informationen der Telekom zufolge seien Komponenten eines britischen TK-Provider erfolgreich infiziert worden.

Beim Vorfall handelt es sich um ein meldepflichtiges Ereignis nach TKG/IT-SiG. Die Meldung durch BNetzA ggü. BSI erfolgte unvollständig/ anonymisiert nach zwei Tagen und rechtskonform/vollständig erst nach fünf Tagen.

Maßnahmen und weiteres Vorgehen:

Nach Bekanntwerden des Vorfalls wurde die Öffentlichkeit umgehend durch die DTAG, BMI und BSI informiert.

Das BKA hat gemeinsam mit der SA Köln die Ermittlungen aufgenommen. Die Ermittlungen dauern an. Das BfV ermittelt im Rahmen seiner Zuständigkeit. (Anmerkung: Zur Sitzung wurde auch ein Vertreter des BfV eingeladen. Da die Ermittlungen noch andauern, sollte der Bitte nicht entsprochen werden.)

Die Telekom hat dem BMI informell mitgeteilt, dass sie i.d.L. gewesen wäre, innerhalb weniger Minuten den Angriff technisch zu unterbinden. Mangels rechtlicher Eingriffsbefugnisse war dies nicht möglich. Die DTAG wird dies mglw. in der Sitzung als politisch erforderlichen Schritt kommunizieren.

7

**4. Gesprächsführungsvorschlag** (max. 1 Seite)

- Ausfälle im Telekom-Netz am 27. und 28.11.2016 durch einen Mirai-Botnet Angriff.
- weltweiter Angriff, der nicht speziell der Telekom galt
- Auch das Regierungsnetz wurde attackiert, aber wegen der vorhandenen Sicherheitsinfrastruktur und zusätzlichen Filtermaßnahmen des BSI nicht kompromittiert.
- ca. 950.000 Router bei Telekomkunden ausgefallen
- BSI hat Bundesverwaltung umgehend gewarnt und Informationen zu Schutzmaßnahmen auch an nicht an den IVBB angeschlossenen Behörden übermittelt
- BKA und Staatsanwaltschaft Köln, sowie BfV ermitteln; zu laufenden Verfahren keine Aussagen. Grundsätzlich kann es sich bei den Tätern um kriminelle Einzeltäter aber auch um staatliche Stellen handeln.
- Der neuartige Vorfall zeigt wie empfindlich unsere Kritischen Infrastrukturen sind.
- Der Schutz der Kritischen Infrastrukturen muss daher weiter gehärtet und bestehende rechtliche Regelungen und Meldewege kritisch hinterfragt und ausgebaut werden.
- Hierbei stellen sich auch Haftungsfragen. Verbraucher müssen auf die Sicherheit der auf dem Markt befindlichen IT-Produkte vertrauen können. Das war hier nicht der Fall. Verantwortung für die digitale Sicherheit tragen Nutzer, Management in Unternehmen und Behörden, Hersteller, Provider und Dienstanbieter gleichermaßen. Das werden wir uns im BMI jetzt genauer anschauen.
- Technische Details zum Vorfall sollten P BSI und Telekom ausführen.

MinR Reisen RAFr Gobel

Bundesamt
für Sicherheit in der
Informationstechnik

# Pressemitteilung

HAUSANSCHRIFT
Godesberger Allee 185 - 189
53175 Bonn

TEL +49 (0) 22899 9582 - 5777
FAX +49 (0) 22899 9582 - 5400

presse@bsi.bund.de
www.bsi.bund.de

## Cyber-Angriffe auf Telekom-Kunden: BSI fordert Umsetzung geeigneter Schutzmaßnahmen

Bonn, 28. November 2016. Am 27. und 28. November 2016 sind über 900.000 Kundenanschlüsse der Deutschen Telekom von Internet- und Telefonieausfällen betroffen gewesen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) steht in ständigem Austausch mit der Deutschen Telekom, um diesen Vorfall zu analysieren.

Das BSI ordnet diesen Ausfall einem weltweiten Angriff auf ausgewählte Fernverwaltungsports zu. Dieser erfolgte, um die angegriffenen Geräte mit Schadsoftware zu infizieren. Diese Angriffe wurden auch in dem vom BSI geschützten Regierungsnetz registriert, in dem sie aber auf Grund funktionierender Schutzmaßnahmen folgenlos blieben. Das Nationale Cyber-Abwehrzentrum koordiniert derzeit unter Federführung des BSI die Reaktion der Bundesbehörden.

„In dem am 9. November vorgestellten Bericht zur Lage der IT-Sicherheit in Deutschland haben wir auf die Gefahren durch Hackerangriffe insbesondere für Kritische Infrastrukturen hingewiesen. In der Cyber-Sicherheitsstrategie wurden bereits geeignete Maßnahmen zum Schutz vor Angriffen auf unsere digitale Infrastruktur beschlossen. Diese müssen nun wirken", erklärte BSI-Präsident Arne Schönbohm.

**Weitere Informationen:**

Bericht zur Lage der IT-Sicherheit in Deutschland

Cyber-Sicherheitsstrategie

**Pressekontakt:**

Bundesamt für Sicherheit in der Informationstechnik
Pressestelle
Tel.: 0228-999582-5777
E-Mail: presse@bsi.bund.de
Internet: **www.bsi.bund.de**

**Referat: ITII2** 29.11.2016

Bearbeiterin: RAFr Gobel Tel. -11993

***Cyber-Angriff auf das Netz der Dt. Telekom***

**Sachstand:**

- Ausfälle im Telekom-Netz durch IoT Mirai-Botnet Angriff (Ziel ist Fernsteuerung der „Bots" (in diesem Fall der Router) durch einen Server zum Zwecke sogenannter Denial-of-Service Angriffe)
- Ziel sind bestimmte Speedport-Router der Dt. Telekom, um Botnet zu erweitern
- ca. 950.000 Kunden mit Geräten des Herstellers „Arcadyan" betroffen
- Botnet-Angriff führt zu keiner Infektion der Geräte, aber zum Absturz
- Angriff ist nach TKG/IT-SiG meldepflichtig

**Reaktion:**

- Eine Reaktion der BNetzA ggü. BSI erfolgte bisher nicht
- BMI und BSI haben über ihre Kontakte zur Telekom umgehend den Sachstand eruiert und Maßnahmen mit der Telekom besprochen

**erfolgte Maßnahmen:**

- Information der Öffentlichkeit
- Netzwerk-Filtermaßnahmen durch die Telekom, um das Netzwerk zu schützen
- Telekom hat gemeinsam mit dem Hersteller „Arcadyan" kurzfristig einen Patch bereitgestellt
- Das BSI hat die Bundesverwaltung umgehend gewarnt und Handreichungen für Portsperrungen übermittelt

**Statement:**

- Die zuständigen Behörden BSI und BMI standen im sofortigen Kontakt mit der Dt. Telekom, um den Vorfall, Vorgehen und Auswirkungen zu besprechen.
- Der neuartige Vorfall zeigt, wie empfindlich unsere Kritischen Infrastrukturen sind.
- Wir werden im Sinne des IT-Sicherheitsgesetzes den kooperativen Gedanken aufgreifen und dafür sorgen, dass der Schutz der Kritischen Infrastrukturen weiter gehärtet wird.

**Referat: ITII2** 29.11.2016

Bearbeiterin: OAR Pletat Tel. -10381

***Cyber-Angriff auf das Netz der Deutschen Telekom***

**Sachstand:**

- Ausfälle im Telekom-Netz durch IoT Mirai-Botnet Angriff (Ziel ist Fernsteuerung der *„Bots" (in diesem Fall der Router der Telekom-Kunden) durch einen Server insb.* zum Zwecke sogenannter Denial-of-Service Angriffe)
- Ziel sind bestimmte Speedport-Router der Dt. Telekom, um Botnetz zu erweitern
- ca. 950.000 Kunden mit Geräten des Herstellers „Arcadyan" betroffen
- Botnet-Angriff führt zu keiner Infektion der Geräte, aber zum Absturz
- Angriff ist nach TKG/IT-SiG meldepflichtig
- Funktionalität im Netz der Telekom, bis auf Einzelfälle, wiederhergestellt
- Regierungsnetze wurden zwar attackiert, aber wegen Filtermaßnahmen des BSI ohne Erfolg

**Meldewege:**

- Eine Reaktion der BNetzA ggü. BSI erfolgte erst nach zwei Tagen und unvollständig
- BMI und BSI haben über ihre Kontakte zur Telekom umgehend den Sachstand eruiert und Maßnahmen mit der Telekom besprochen.

**Erfolgte Maßnahmen:**

- Information der Öffentlichkeit
- Netzwerk-Filtermaßnahmen durch die Telekom, um das Netzwerk zu schützen
- Telekom hat gemeinsam mit dem Hersteller „Arcadyan" kurzfristig einen Patch bereitgestellt
- Das BSI hat die Bundesverwaltung umgehend gewarnt und Handreichungen für Portsperrungen übermittelt
- Vorbereitung eines Interviews von Herrn Minister mit der Bild - Zeitung (anbei)