Schlagabtausch zu ZITiS: IT-Sicherheitslücken schließen oder ausnutzen?

Originalartikel

Backup

<html> <p class=„printversionback-to-article printversion–hide“>zurück zum Artikel <figure class=„printversionlogo“></figure><figure class=„aufmacherbild“><figcaption class=„akwa-caption“><p class=„source akwa-captionsource“>(Bild: pixelcreatures) </figcaption></figure> Macht die staatlicher Hack-Behörde ZITiS uns sicherer oder leistet sie der IT-Sicherheit einen Bärendienst? Darüber stritten ZITiS Präsident Wilfried Karl und der Bundesdatenschutzbeauftragte a.D. Peter Schaar beim Domain Pulse in München. Auf „verfassungsrechtlich dünnem Eis“ bewegt sich die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) nach Ansicht von Peter Schaar. Der ehemalige Bundesbeauftragte für den Datenschutz sprach beim Domain Pulse[1], der Konferenz der deutschsprachigen Domain Registries, von einer „trügerischen Sicherheit“ durch die neue Staats-Spyware. ZITiS-Präsident Wilfried Karl verteidigte das Mandat seiner Behörde und versicherte, im Normalfall würden Schwachstellen doch geschlossen. <figure class=„rteinlinebild akwa-inline-img rtepos_right col-lg-6 col-md-6 col-sm-6 col-xs-12 akwa-inline–right“><figcaption class=„rteinlinebild_source akwa-caption“>Wilfried Karl (links) und Peter Schaar (rechts) während der Debatte (Bild: Monika Ermert/heise online)</figcaption></figure> Schaar kritisierte die enorme Ausweitung der Befugnisse für die Sicherheitsbehörden, die von der alten Großen Koalition aus CDU/CSU und SPD massiert in den vergangenen zwei Jahren auf den Weg gebracht worden war. 17 von 35 neuen Überwachungsgesetzen stammen aus dieser Zeit: von der Legalisierung der BND-Praktiken zur präventiven Ausspähung von Datenverkehren über den Zugriff aller Bundesbehörden auf die bei den Einwohnermeldeämtern gespeicherten biometrischen Daten der Bürger bis hin zum Staatstrojaner und zum ewigen Wiedergänger Vorratsdatenspeicherung. Die Aufgabe des neu aufgebauten ZITiS, Sicherheitslücken gleichermaßen für den Verfassungsschutz, Polizei und Strafermittler zu besorgen, sorgt nach Schaars Ansicht gerade nicht für mehr Sicherheit, sondern kompromittiere diese. „Die Aufbewahrung von Sicherheitslücken halte ich für ein problematische Thema“, sagte er im Steitgespräch zu Karl, „insbesondere, wenn sie länger aufbewahrt werden.“ Würde man sagen, „OK, nach zwei Wochen ist Schluss“, könnte sich der Bundesdatenschützer a.D. eher anfreunden mit der Idee: „Aber solche Vorgaben gibt es nicht“. <h3 class=„subheading“ id=„nav_fehlende1“>Fehlende gesetzliche Grenzen</h3> Weil die Bundesregierung bei der Errichtung des ZITiS auf ein gesetzliche Grundlage verzichtet hatte, fehlen laut Schaar generell klare Grenzziehungen dafür, was das ZITiS eigentlich darf und was nicht. Im dürren Ministererlass[2] zur Einrichtung fehlten

beispielsweise Richtlinien darüber, ob und wie das ZITiS verhindern müsse, dass die gemeinsam für Geheimdienstler und Strafverfolger entwickelten Werkzeuge am Ende über das gesetzlich vorgesehene Maß hinaus eingesetzt würden. Die Aufhebung der Trennung zwischen geheimdienstlicher und polizeilicher Arbeit nannte Schaar eine Grauzone und verfassungsrechtlich höchst bedenklich. Das Verhältnis von ZITiS, das Schwachstellen beschaffen, und des Bundesamts für Sicherheit in der Informationstechnik (BSI), das die Schwachstellen schließen soll, bleibe vage. <h3 class=„subheading“ id=„nav_kriterienkatalog2“>Kriterienkatalog für Behandlung von Schwachstellen nötig</h3> Karl anerkannte in dem Streitgespräch, das Ausnutzen von Schwachstellen stelle die Behörden vor „einen Zwiespalt zwischen der Schließen von Sicherheitslücken und der Frage, kann ich sie, meist auch nur temporär zum Nutzen für staatliche Überwachungszwecke offenhalten“. Natürlich würden die Behörden damit verantwortungsvoll um gehen, hielt der Behördenchef Schaar entgegen. Trotzdem ist es seiner Meinung nach notwendig, einen Prozess zu etablieren, der klarstellt, wie man jeweils mit den einzelnen Schwachstellen umgehen soll. Zu den Kriterien, die dabei vor der Entscheidung „ausnutzen oder schließen“ zu berücksichtigen sind, gehört laut Karl weniger der Verbreitungsgrad als „wie schwerwiegend wären die Auswirkungen“ und „bei welchen Systemen kommt diese Sicherheitslücke zur Anwendung“. Außerdem sei zu prüfen, wie leicht sie auszunutzen ist. „Kann ein Schüler mit ersten Informatikkenntnissen das oder braucht man die Ressourcen eines großen staatlichen Akteurs“, fragte Karl und versicherte schließlich: „Der Normalfall wird immer sei, dass man seine solche Lücke schließen wird.“ Daran arbeiteten im übrigen ja auch tausende von privaten Sicherheitsforschern und Organisationen weltweit. Die Erstellung eines Kriterien- und Verfahrenskatalogs für die Behandlung der Schwachstellen müsse, so Karl, von den zuständigen Ministerien angestoßen werden. „Das ZITiS kann das nicht allein machen.“ <h3 class=„subheading“ id=„nav_bisher_nur3“>Bisher nur Leute eingekauft</h3> Gleichzeitig warnte er, das ZITiS auf die Aufgabe Schwachstellenanalyse zu reduzieren. Man unterstütze Bundeskriminalamt, Bundespolizei und Bundesamt für den Verfassungsschutz vor allem auch in Sachen Telekommunikationsüberwachungstechnik allgemein, sowie Kryptoanalyse und Analyse von Big Data. Bei der Schwachstellen Beschaffung hat man laut Karl übrigens das „hehre Ziel“, in Zukunft „möglichst 100 Prozent der Schwachstellen“ selbst aufzuspüren. Doch bis man soweit ist, müsse man sich wohl auch auf dem Markt umschauen, sagte Karl gegenüber heise online. Bislang habe man noch keine Schwachstellen eingekauft, sagte Karl. Noch stehen Anforderungen von den Bedarfsträgern, also den Strafverfolgern und Geheimdiensten, aus. Für 2018 ist man vor allem am Einkauf von Mitarbeitern interessiert. Aktuell hat die Behörde 30 der zunächst vorgesehenen 120 Mitarbeiter, für 25 weitere seien Arbeitsverträge bereits unterschrieben (Monika Ermert) / (mho[3])<br class=„clear“/> <hr/> URL dieses Artikels:
<small>

```
http://www.heise.de/-3976587
```

</small> Links in diesem Artikel:
<small>

```
<strong>[1]</strong>&amp;#160;https://www.domainpulse.de/de/programm
```

</small>
<small>

```
<strong>[2]</strong>&amp;#160;https://wiki.freiheitsfoo.de/pmwiki.php?n=Main.ZIT
```

```
iS#toc44
```

</small>
<small>

```
<strong>[3]</strong> mailto:mho@heise.de
```

</small>
 Copyright © 2018 Heise Medien </html>