

Stellungnahme des Fachschaftsrats Informatik zu den neuen Entwicklungen beim Frühwarnsystem

Sehr geehrte Studentenschaft, Professoren, Mitarbeiter und sonstige Betroffene,

seit dem Frühjahr beschäftigt sich der FSR Informatik mit dem geplanten Frühwarnsystem (FWS) der TU Dresden.

Wir legen Wert darauf, dass bei der Lösung von IT-Problemen die Persönlichkeitsrechte der Nutzer gewahrt werden. Der erste „Entwurf für eine Betriebsordnung eines Frühwarnsystems“ erlaubte die Speicherung persönlicher Daten in unseres Erachtens unnötig hohem Umfang. Der Zugriff auf diese Daten war unzureichend geregelt.

Die Verantwortlichen, Mitarbeiter des ZIH und der Datenschutzbeauftragte der TU Dresden, nahmen sich für einen konstruktiven Dialog mit uns Zeit und erarbeiteten einen Kompromiss, der sowohl die Interessen des ZIH (Nutzung des Systems zur Erhöhung der Netzwerksicherheit), als auch Nutzerinteressen (Zugriff auf die Daten, unabhängige Kontrolle) besser regelte.

Jedoch konnten wir unsere Forderungen nach der Streichung weiterer Zwecke neben „Erkennung und Beseitigung von Störungen / Gewährleistung des ordnungsgemäßen Systembetriebs“ nicht durchsetzen. Unsere Auffassung, dass die Daten nicht für Zwecke wie „Forschung und allgemeine Informationszwecke“ genutzt werden dürften, wurde von den Verhandlungspartnern nicht geteilt.

Daher hatten wir am 07.05.2009 den sächsischen Datenschutzbeauftragten um eine rechtliche Einschätzung der Betriebsordnung gebeten. Diese ist vor kurzem bei uns eingetroffen und unter einzusehen.

Generell ist der Betrieb eines Intrusion-Detection-Systems rechtlich möglich, die anfallenden Daten dürfen aber nur für stark eingegrenzte Zwecke genutzt werden. Der Zugriff ist entsprechend zu regeln.

Anzuwendendes Recht

Mehrere Rechtsordnung spielen beim Betrieb eine Rolle, je nachdem wer die IT für welches Vorhaben nutzt.

In Bezug auf die studentische Nutzung gilt die SächsStudDatVO, da die entsprechend notwendige Rechtsverordnung des SMWK noch nicht existiert.

In Bezug auf die Nutzung durch Mitarbeiter der TU fehlt es an der Ermächtigungsgrundlage, da weder das Sächsische Datenschutzgesetz noch §14 SächsHG Anwendung findet.

In Bezug auf die private Nutzung kann die TU Dresden, als Dienstanbieter nach TKG, personenbezogene Daten zum Erkennen und Beseitigen von Störungen verwenden. Im Rahmen des FWS dürfen die Daten erst bei konkreten Verdacht personenbezogen ausgewertet werden.

Anwendungsziele

Die Betriebsordnung des FWS sieht nach §1 folgende Betriebsmöglichkeiten vor:

- a) Gewährleistung des ordnungsgemäßen Systembetriebs
- b) Ressourcenplanung und Systemadministration
- c) Erkennen und Beseitigen von Störungen
- d) Aufklärung und Unterbindung rechtswidriger und missbräuchlicher Nutzung
- e) Forschung und allgemeine Informationszwecke

Für die Ziele nach Punkt b) und e) darf das FWS nicht eingesetzt werden.

Der "ordnungsgemäße Systembetrieb" nach Punkt a) ist weiter gefasst als das Erkennen und die Beseitigung von Störungen. Es wurde daher vorgeschlagen auch diesen Punkt zu streichen und entsprechende Regelungen nach §§ 88, 100 TKG mit in Punkt c) zu integrieren.

Herr Herber, der Datenschutzbeauftragte der TUD, teilte uns am 16.10.2009 auf Anfrage mit, dass die Änderungsvorschläge des sächsischen Datenschutzbeauftragten „wie empfohlen, bereits umgehend und uneingeschränkt Eingang in die Ordnung gefunden haben“. Wir begrüßen dies sehr und möchten uns an dieser Stelle erneut bei den Verantwortlichen für die konstruktive Zusammenarbeit bedanken und nochmals darum bitten, uns bei ähnlichen Planungen eher einzubeziehen.

Weiterhin bestätigte Herr Herber erneut, dass das FWS derzeit noch nicht in Betrieb ist.

Zusätzlich zur rechtlichen Situation des FWS wird die „Geeignetheit und Erforderlichkeit in datentechnischer Hinsicht“ derzeit noch vom Technikreferat des Sächsischen Datenschutzbeauftragten geprüft.

Für Rückfragen steht der FSR Informatik gerne per Mail an fsr@ifsr.de oder persönlich zur Verfügung.