Christian-Albrechts-Universität zu Kiel, 24098 Kiel

An alle Administratoren und
Systemverwalter von PC-Systemen
der Zentralen Verwaltung
der Dekanate
der Institute/Seminare
hier

Kanzler
Dr. Oliver Herrmann

Hausanschrift:
Christian-Albrechts-Platz 4, 24118 Kiel

Postanschrift: 24098 Kiel

www.uni-kiel.de

Bearbeiter/in, Zeichen
Claus Frömsdorf
110

Mail, Telefon, Fax
cfroemsdorf@uv.uni-kiel.de
tel +49(0)431-880-3005
fax +49(0)431-880-7333

Datum
28. September 2006

Verhaltensempfehlungen bei polizeilichen Ermittlungen

Sehr geehrte Damen und Herren,

vom Rechenzentrum wurden Verhaltensempfehlungen erarbeitet, die ich Ihnen in der Anlage zur Kenntnis gebe. Ich bitte diese Hinweise unbedingt zu beachten, damit die Arbeit der Polizei nicht behindert wird.

Mit freundlichen Grüßen

Dr. Oliver Herrmann

Verhalten bei Ermittlungen innerhalb der CAU

Einleitung

Immer häufiger wird das Internet für rechtswidrige oder gar kriminelle Handlungen genutzt. Dementsprechend kommt es auch immer häufiger vor, dass die CAU das Ziel von Ermittlungsbehörden ist. Zur Klärung der Sachverhalte wird die Mitwirkung von Systemverwaltern erforderlich. Dann stellt sich sehr schnell die Frage, wie man sich richtig verhält, was Rechte und Pflichten sind und wie eine Kooperation im Einzelfall aussehen kann. Einige solcher Fragen sollen im Folgenden aufgeworfen und behandelt werden. Dieses Papier richtet sich hauptsächlich an Systemverwalter, kann aber sicher auch für andere Personen von Bedeutung sein.

Ausgangslage

1. Die CAU duldet keine Straftaten, die unter Nutzung ihrer Infrastruktur begangen werden. Sie unterstützt im Rahmen der geltenden Gesetze die Ermittlungsbehörden bei ihrer Arbeit nach besten Kräften.

2. Die Zahl der Delikte steigt erheblich, damit auch die Zahl der Ermittlungen. Die Delikte kommen hauptsächlich aus folgenden Bereichen:
   - Verletzung des Urleberrechts (z.B. Download/Upload von MP3-Musikdateien oder Videos)
   - Betrug
   - Kinderpornographie (hier ist schon der Besitz strafbar!).

3. Wenn solche Straftaten von einem Rechner aus dem Bereich der CAU begangen werden, kann es sich grundsätzlich immer handeln um:
   - Vorsatz des Systembetreuers
   - Vorsatz des Besitzers/Anwenders des Systems oder eines Accounts
   - gehackte Systeme (also ohne Beteiligung eines Mitglieds der CAU).

Problematik

1. Systemverwalter sind aufgrund ihrer allgemeinen Fachkenntnisse und ihrer speziellen Kenntnisse über die von ihnen betreuten Systeme prädestiniert, bei Ermittlungen hinzugezogen und z.B. zur Herausgabe von Geräten oder Informationen aufgefordert zu werden. Dieses kann sie auf (zumindest für sie) rechtlich unsicheres Gebiet führen.

2. Systemverwalter verfügen andererseits über Privilegien und sind somit grundsätzlich dazu in der Lage, die betreuten Systeme für Straftaten einzurichten bzw. zu nutzen und unter Umständen Spuren zu verwischen. Bei Ermittlungen unterliegt ihr Handeln daher einer besonderen Aufmerksamkeit.

3. Bei ungeschicktem oder fehlerhaftem Verhalten besteht für Administratoren bzw. Besitzer eines Systems die Gefahr, selbst in Verdacht zu geraten (z.B. durch versehentliche Zerstörung oder Veränderung von Beweismitteln). Hierzu gibt es Präzedenzfälle, die Konsequenzen können für die Betroffenen äußerst unangenehm sein. Daher sollten bestimmte Handlungsvorgaben im eigenen Interesse unbedingt eingehalten werden.

Allgemeine Informationen und Handlungsgrundsätze

Die im Folgenden aufgeführten Informationen und Handlungsgrundsätze sollen helfen, sich bei der Unterstützung von Ermittlungsbehörden richtig zu verhalten und damit Fehler zu vermeiden.

1. Der Adressat von Ermittlungen ist zunächst immer die CAU als Institution. Sie wird vertreten durch den Kanzler. Sollten sich Ermittler unmittelbar an Administratoren, Besitzer oder Nutzer eines Systems wenden, so ist unbedingt eine sofortige Abstimmung der weiteren Vorgehensweise mit dem Kanzler und der Institutsleitung vorzunehmen und das Rechenzentrum zu informieren.

2. Durchsuchungen und Beschlagnahmungen bedürfen i.d.R. eines richterlichen Beschlusses. Dieser ist von den Ermittlern in Schriftform vorzulegen. Die Ermittler müssen sich ausweisen. Auch in solchen Fällen sind der Kanzler, die Institutsleitung und das Rechenzentrum sofort zu informieren und die weitere Vorgehensweise abzustimmen.

3. Mitarbeiter im öffentlichen Dienst haben Stillschweigen über dienstliche Angelegenheiten zu bewahren. Selbst bei Vorliegen eines richterlichen Durchsuchungs- oder Beschlagnahmebeschlusses ist für Zeugenaussagen eine Genehmigung des Kanzlers erforderlich. Lassen Sie sich insbesondere die Herausgabe von Beweismitteln ausdrücklich genehmigen. Informieren Sie hierüber ebenfalls Ihre Institutsleitung.

4. Geben Sie schriftliche Informationen stets nur über den Dienstweg „im Auftrag" heraus. Sprechen Sie im Zweifelsfall die von Ihnen beabsichtigten Maßnahmen mit der Instituts- oder Universitätsleitung ab.

5. Schalten Sie sofort das Rechenzentrum ein. Hier sind u.U. zusätzlicher Sachverstand oder Erfahrungen aus anderen Fällen vorhanden. Das Rechenzentrum wird mit Ihnen und ggf. in Abstimmung mit den Ermittlern das Beweismaterial nach den üblichen Regeln sichern. Soweit möglich und erforderlich wird das Rechenzentrum das Material unter Verschluß nehmen und die weiteren Schritte veranlassen und koordinieren.

6. Halten Sie stets und unbedingt das 4-Augen-Prinzip ein! Das gilt insbesondere hinsichtlich der Sicherung von Beweismaterial. Denken Sie daran, dass Sie dabei durch Fehler oder Unkenntnis das Material vernichten könnten. Schon das Herunterfahren oder Neustarten eines Rechners verändert Daten!
   Das Rechenzentrum garantiert als „außenstehende" Organisation beim 4-Augen-Prinzip u. U. eher eine neutralere Position, als es z.B. bei einem engen Kollegen gesehen wird. Bedenken Sie stets: Fehler im Umgang mit Beweismitteln könnten als Vorsatz interpretiert werden und Sie als Person in Verdacht geraten lassen. Fertigen Sie stets ein Protokoll an, das mindestens von zwei Personen abgezeichnet wird.

7. Unternehmen Sie niemals Ermittlungen auf eigene Faust, auch nicht um den Ermittlern zu helfen.

8. Gehen Sie stets offen mit den Ermittlern um und versuchen Sie nicht, etwas zu verheimlichen, selbst wenn im Zuge der Beweissicherungen Verstöße gegen andere Rechtsvorschriften (wie z.B. gegen den Datenschutz) offenbar werden.