



## Rundschreiben des Rechenzentrums

Erzstraße 51  
D-38678 Clausthal-Zellerfeld  
Tel.: 05323/72-2045

---

Alle Fakultäten und wissenschaftliche Einrichtungen  
Zentrale Einrichtungen  
Präsidialbüro  
Verwaltung  
Personalrat  
Gleichstellungsbüro

H i e r

24. Mai 2012

---

## Maßnahmen zur Erhöhung der Netzwerksicherheit und Stabilität

Sehr geehrte Damen und Herren,

die Sicherheitsanforderungen an die IT in den Instituten wachsen stetig. Dies liegt u.a. an den steigenden Gefahren durch Viren, Trojaner und andere Schad-Software, aber auch an den Gefahren durch Industriespionage und Diebstahl geistigen Eigentums. In vielen Instituten besteht gegenüber Projektpartnern sogar die Verpflichtung, gesammelte Daten gegen unautorisierten Zugriff zu schützen.

Das Ziel des Rechenzentrums ist es, für Ihre Einrichtung ein IT-Umfeld zu schaffen, in dem die Anzahl der Angriffsvektoren auf Ihre IT-Systeme so weit wie möglich reduziert wird. Dies erreichen wir durch die Betreuung durch die IT-Cluster und andere organisatorische Maßnahmen, aber auch durch technische Maßnahmen wie Firewalling, zentrale, hochverfügbare Datenspeicher und zentral verwaltete Authentisierung.

Ein großes Angriffspotential bietet das lokale Netzwerk Ihres Institutes bzw. Ihrer Einrichtung. Ein Angriff auf Ihre Systeme über das Netzwerk erfordert keinen physischen Zugriff auf die Hardware und birgt aus diesem Grund erhebliche Gefahren. Dies gilt ganz besonders für vernetzte Systeme, die ohne das Wissen der IT-Verantwortlichen einer Einrichtung ans Netz angeschlossen werden (z.B. unautorisiert mitgebrachte Laptops). Diese können hinter Schutzeinrichtungen wie Firewalls agieren und entziehen sich so Schutzmaßnahmen, die normalerweise zuverlässig Angriffe über das externe Netz abwehren.

Hier möchten wir Ihnen zwei Lösungen anbieten, die die Sicherheit im Netz Ihrer Einrichtung deutlich erhöhen: „**DHCP-Snooping**“ und „**802.1X**“

DHCP ist ein wichtiger und weit verbreiteter Service, mit dem Computer automatisch in das Netzwerk eingebunden werden. Gleichzeitig erlaubt der Dienst mit Hilfe des Mechanismus **DHCP-Snooping** in den Netzwerkverteilern die Kontrol-

le, welche Geräte in das lokale Netz eingebracht werden. Deshalb werden die IT-Cluster-Administratoren in den kommenden Wochen auf Sie zukommen und Ihnen dabei helfen, Ihre IT – wo möglich und sinnvoll – auf DHCP umzustellen.

Eine weitere Sicherheitsstufe wird mit der Authentifizierung und Autorisierung nach dem **802.1X**-Verfahren angeboten. Auch hier werden wir zeitnah mit Ihnen absprechen, ob Ihr Bereich dafür geeignet ist.

Beide Maßnahmen sind wichtige Schritte, um die Sicherheit im Hochschulnetz weiter zu erhöhen, und wir hoffen auf eine gute Zusammenarbeit bei der Umsetzung der TUC-übergreifenden Sicherheitsstrategie.

Mit freundlichen Grüßen

gez. C. Strauf (Leiter Netzabteilung)