Sicherheitsratschläge für Benutzer des CIP-Pools der Fakultät für Physik

Maximilian Imgrund, Rechnerbetriebsgruppe

28. Juni 2011

Zusammenfassung

Wir haben festgestellt, dass beim alltäglichen Arbeiten im CIP einerseits aus Unkenntnis, andererseits aus Fahrlässigkeit diverse Sicherheitsaspekte nicht beachtet werden. Dieses Dokument möchte dem unerfahrenen Benutzer die Informationen an die Hand geben, die frühere Fehler verhindern sollen. Neben Grundlagen zum Passwortschutz geht das Dokument auch näher auf spezifische Eigenschaften der Rechnersysteme ein und erklärt, wie der Benutzer sich und andere effektiv vor Accountmissbrauch und Datenklau schützen kann.

Inhaltsverzeichnis

1 Der Campusaccount

Mit der Vereinheitlichung der Authentifikationstruktur sind viele Prozesse einfacher geworden. Der Benutzer kann mit einem einzigen Login auf umfangreiche Dienste zurückgreifen. Dazu gehören diverse Verwaltungsmechanismen, wie Klausuranmeldung und Studiengebührenkonto, E-Mail-Konten, Die Campus-Infoseite, virtuelle Seminarräume, Computerarbeitsplätze in den Bibliotheken und Fakultäten sowie VPN-gesicherter WLAN-Zugriff. Dies ist auf der einen Seite natürlich sehr komfortabel, andererseits birgt die Tatsache, dass ein Login

für sämtliche Bereiche und Funktionen den Benutzer identifiziert, auch Risiken. Die Sicherheit dieses Systems steht und fällt mit der Geheimhaltung dieses einen Passwortes. Daher sollte man die im Folgenden sicherlich bekannten, aber oft missachteten Regeln einhalten, um zu verhindern, dass Dritte an sensible Daten gelangen oder mit einer gestohlenen Identität Missbrauch treiben:

- *Wählen Sie kein einfaches Passwort*, denn ein einfaches Passwort ist schnell geraten. Das Passwort sollte mindestens 8 Zeichen lang sein, und am Besten Groß- und Kleinschreibung ebenso wie Ziffern beinhalten. Am denkbar ungünstigsten sind Wörter, die in einem Wörterbuch zu finden sind, Leerzeichen, Eigennamen und Bezeichnungen oder Beschriftungen von Gegenständen in Reichweite.

- *Wählen Sie kein Passwort, das Sie bereits für etwas anderes benutzen.* Denn während das Passwort hier sicher verschlüsselt ist, muss das nicht für Dienste von Drittanbieter gelten. Das Mailpasswort wird zum Beispiel bei einigen Freemail-Providern unverschlüsselt übertragen und ist somit leicht abhörbar.

- *Schreiben Sie ihr Passwort nie auf.*

- *Lassen Sie sich nicht über die Schulter sehen.* Gerade dies ist eine einfache Methode, wie andere an Ihr Passwort kommen. Sie schauen einfach beim Tippen zu. Achten Sie darauf, dass Sie bei Eingabe des Passwortes nicht beobachtet werden.

- *Ändern Sie ihr Passwort regelmäßig.* Denn auch dies ist eine effektive Methode, Trittbrettfahrer abzuschütteln. Ändern können Sie ihr Passwort auf der Internetseite von $Campus^{LMU}$[1].

- *Geben Sie Ihr Passwort NIE an Dritte weiter:* Mag es auch die Freundin oder der Freund sein, sie sollten auch hier keine Ausnahme machen. Es kommt immer wieder vor, dass sich Dritte mit den Daten anderer anmelden. Wenn sie auch von Ihnen autorisiert sein mögen: Sie kennen im Allgemeinen die Sicherheitsrichtlinien nicht und neigen eher dazu, unvorsichtig mit dem Passwort umzugehen (es beispielsweise aufzuschreiben, weil sie es sich nicht merken können, um dann anschließend versehentlich den Zettel liegen zu lassen).

Wir möchten im Zusammenhang mit dem letzten Absatz erwähnen, dass dieser auch in den Benutzungsrichtlinien des LRZ[2] unter §4.3 fest vorgeschrieben ist. Sogenanntes *Social Engineering* zielt genau auf diesen Punkt ab. Der Benutzer wird unter einem Vorwand über sensible Daten wie Passwörter, Sicherheitsmechanismen oder Netzwerkstruktur ausgefragt und gibt relevante Daten versehentlich und nichts ahnend preis.
Des Weiteren könnten Sie von Dritten auch per E-Mail oder Web nach ihren Daten gefragt werden (sog. *Phishing*). Dabei wird oft eine offiziell erscheinende Mitteilung verschickt, die auf ein echt erscheinendes Formular verlinkt oder direkt nach Ihren Zugangsdaten fragt. Die Rechnerbetriebsgruppe und das LRZ

[1] http://campus.lmu.de
[2] http://www.lrz-muenchen.de/wir/regelwerk/benutzungsrichtlinien

wird nie eine solche Aufforderung an Sie richten. Wenn Sie eine solche Mail bekommen oder auf eine derartige Website stoßen, benachrichtigen Sie uns bitte unverzüglich, Sie sind vielleicht nicht der Einzige Betroffene.

2 Der CIP-Pool der Fakultät für Physik

2.1 An- und Abmelden an den Rechnern

Wie Sie sicherlich bereits wissen, können Sie sich lokal an unseren Rechnern unter Angabe des Campuslogins ohne @campus.lmu.de anmelden. Bereits hier könnte ein Angreifer an ihre Logindaten gelangen: Er blendet eine falsche Anmeldemaske ein, welche die Logindaten an ihn sendet. Schauen Sie also genau hin, ob es sich um den üblichen Anmeldeschirm handelt und geben Sie Ihre Logindaten nicht ein, falls Sie Zweifel an der Echtheit der Anmeldung haben. Es gibt eine einfache Methode sich gegen einen solchen Angriff abzusichern. *Drücken Sie STRG+ALT+DRUCK+K, um die Grafische Oberfläche neu zu starten.* Der Bildschirm wird kurz schwarz um darauf den echten Loginbildschirm anzuzeigen. Mit dieser Tastenkombination können Sie sich im Übrigen ebenso bei einem Absturz neu einloggen oder einen Abmeldevorgang, der hängen geblieben ist, schnell beenden. Vom regulären Gebrauch der Funktion ist abzusehen, da diese alle Programme schließt, ohne diesen Zeit zu geben, beim Beenden Daten zu sichern.
Sie sollten sich, damit nach Ihnen niemand Ihren Account benutzt, *immer abmelden.* Dies gilt insbesondere für die unter STRG+ALT+(F1 bis F6) erreichbaren Textkonsolen, da diese sich bei Untätigkeit nicht automatisch sperren.
Wenn Sie längere Berechnungen ausführen möchten und nicht dabeisitzen wollen, so bitten wir, der RBG Bescheid zu geben. Andernfalls werden wir nach einigen Stunden nach eigenem Ermessen Ihre Programme schließen und Sie abmelden um den Rechner wieder voll für andere verfügbar zu machen.

2.2 Drucken

Sie haben im CIP einen Semesterfreibetrag von 18 Euro , den Sie für Ausdrucke verwenden können. Da in der Theresienstraße auch noch einige Computerarbeitsplätze und Drucker eingerichtet sind, sollten Sie *immer darauf achten, an welchen Drucker Sie Ihren Druckauftrag richten.* Das spart Ihnen Zeit, Guthaben und den Weg zum anderen Drucker. Holen Sie Ihre Ausdrücke immer sofort ab und geben Sie besonders auf persönliche oder vertrauliche Dokumente acht, da die Drucker frei zugänglich sind. Es passiert häufig, dass persönliche Daten am falschen Drucker gedruckt oder nicht abgeholt werden. Die RBG behält sich vor, solche sensiblen Dokumente bei Nichtabholung zu vernichten oder im Administrationsraum aufzubewahren. Falls Sie einen Ausdruck vermissen, fragen Sie einfach im Administrationsraum nach.

2.3 Datenhaltung und Rechtevergabe

2.3.1 Rechtevergabe in Linux

Sie arbeiten, wenn Sie sich im CIP anmelden, an einem sogenannten *Mehrbenutzersystem*. Das bedeutet, dass einerseits mehrere Benutzer sich an einem Rechner anmelden können(Textkonsolen, SSH, grafische Konsolen etc.), andererseits, dass Sie sich mit den anderen die Ressourcen(CPU,Festplatte,Netzwerk) teilen. Linux verfügt über ein ausgeklügeltes Sicherheitsmodell. Dennoch sollten Sie unbekannte Dateien aus dem Netz nicht ausführen und nicht öffnen. Zwar gibt es wenige Viren für Linux und die Wahrscheinlichkeit für einen Schaden am ganzen System ist gering; Ihre eigenen Daten können aber sehr wohl durch Viren und Trojaner beschädigt werden. Es gilt also dieselbe Sorgfalt zu wahren wie unter Windowssystemen.
Die Rechte sind hier im CIP standardmäßig so eingerichtet ist, dass andere Benutzer die Daten in Ihrem Heimverzeichnis nicht einsehen können. Durch Bedienungsfehler ist es aber möglich, dass Sie den anderen Benutzern die Rechte geben, Ihre Dateien einzusehen.
Die Verzeichnisse */tmp und /large_tmp sind für alle schreib- und lesbar*. Es handelt sich um Verzeichnisse für Daten, die Programme temporär brauchen aber nicht dauerhaft speichern wollen. Programme schützen die Daten, die sie dort ablegen durch korrekt einschränkende Rechtevergabe. Wenn Sie hingegen Daten nach /tmp oder /large_tmp kopieren, ohne die Rechte einzuschränken, so sind sie für alle anderen Benutzer des Systems lesbar.
Darum *Arbeiten Sie nie in den temporären Verzeichnissen*[3]
Auch Ihr Heimverzeichnis ist so sicher, wie Sie es anlegen. folgen Sie den Anweisungen, um ihre Dateien nur für sie schreibbar und lesbar zu machen. Öffnen Sie eine Konsole(z.B. durch Drücken von ALT+F2 und Ausführen des Befehls konsole oder xterm). Sie können mit dem Befehl

```
ls -l ~
```

die Dateien in ihrem Heimverzeichnis anzeigen. “ls -l” ist dabei der Befehl die Dateien in einem Verzeichnis aufzulisten, “~” steht immer symbolisch für Ihr Heimverzeichnis. Der Befehl zeigt eine dem Folgenden ähnelnde Ausgabe an:

```
 total 1228
drwx------ 2 Maximilian.Imgrund campususer   4096 2007-09-13 13:10 bin/
drwx------ 2 Maximilian.Imgrund campususer   4096 2008-06-19 14:30 Desktop/
drwx------ 2 Maximilian.Imgrund campususer   4096 2008-05-17 19:30 Documents/
```

Jede Datei hat einen Besitzer und eine Gruppe(Um mehreren Benutzern Zugriff zu einer Datei zu geben), abzulesen in Spalte 3 und 4. Dabei ist besonders die erste Spalte für unsere Zwecke interessant. Sie zeigt die Rechte der verschiedenen Parteien an. Dabei steht das erste Zeichen für die Funktion der Datei, dann kommen 3x3 Rechtezeichen.

- “d” steht für Directory, also ein Verzeichnis.
- Von den 3x3 Zeichen stehen...

  ...die ersten drei für die Rechte des Besitzers

[3] Ausgenommen von dieser Regel ist der Posterdruck, bei dem wir gerade nutzen, dass der Admin in den Temporären Verzeichnissen auch lesen kann, um das Poster zu drucken.

...die zweiten drei für die Rechte der Gruppe

...und die dritte für die Rechte beliebiger Nutzer

- In den 3 Dreiergruppen steht...

  ..."r" für read, also lesen

  ..."w" für write, schreiben

  ..."x" für execute, also ausführen

Bei normalen Dateien steht Ausführen für ein Programm, bei Verzeichnissen dafür, ob man in die Verzeichnisse absteigen darf. Lesen und schreiben meint bei Verzeichnissen, ob der Benutzer den Inhalt auflisten darf und ob er Dateien anlegen oder löschen darf.
Im Folgenden möchten wir unser Heimverzeichnis exklusiv uns zugänglich machen. Zur Rechtevergabe gibt es das Programm chmod. Folgender Befehl macht Ihr Heimverzeichnis nur noch für Sie schreib-, les- und anzeigbar:

```
chmod -R go-rwx ~
```

Dabei steht "R" für recursive, was das Programm anweist, nicht nur das Zielverzeichnis zu bearbeiten, sondern auch alle anderen Dateien und Verzeichnisse, die sich in ihm befinden , "g" und "o" für group, Gruppe und o, others (nicht zu verwechseln mit u, User, dem eigentlichen Besitzer). Das "-" steht dafür, die nach dem Minus folgenden Rechte abzuerkennen, die da sind :"rwx" , also lesen, schreiben, ausführen. Zuletzt ist das Zielverzeichnis angegeben, welches wieder das Heimverzeichnis ist.
Sie können den Erfolg des Kommandos wiederum mit "ls -l" überprüfen.
Nur als Tipp: Mit

```
man <befehlsname>
```

können Sie die oft präzise und ausführlich geschriebene Dokumentation zu einem Konsolenbefehl oder Programm aufrufen.

2.3.2 Datentransfer

Sie können neben der lokalen Anmeldung sich auch von zu hause aus per SSH auf den Universitätsrechnern einloggen. Die Authentifikation und *Kommunikation über SSH ist verschlüsselt* und ein sicherer Weg, Daten vom CIP zu hause zu nutzen oder von zu hause ins CIP zu übertragen. Zu diesem Zweck gibt es diverse kostenlose Werkzeuge für Windows. Unter Linux sind in der Regel die Standardwerkzeuge SSH,SCP und RSync bereits installiert. Wenn es Ihnen möglich ist, sollten Sie diesen Weg dem Senden per E-Mail vorziehen, da E-Mails im Allgemeinen unverschlüsselt versendet werden und gerade für große Datenmengen nicht geeignet sind.
Vergessen Sie nie, dass es sich bei Daten aus dem Münchner Wissenschaftsnetz, von Lehrstuhlservern oder unseren Servern um nicht öffentliche Daten handeln kann und gehen Sie dementsprechend sorgsam damit um. *Unterlassen Sie insbesondere eine Wiederveröffentlichung*, zum Beispiel durch Kopieren in ihren ungeschützten Homepageordner.
Suchen Sie nach einem Weg einem anderen Benutzer eine Datei zu überspielen, so kopieren Sie diese in das /large_tmp Verzeichnis und lassen den Benutzer

eine Kopie davon anfertigen. Danach löschen Sie die Datei wieder aus dem /large_tmp Verzeichnis. Direkter und sicherer geht es aber mit dem folgenden Kommando:

```
scp beispieldatei.txt Empfänger.Login@rechnername:
```

Dabei sind "beispieldatei.txt" und "Empfänger.Login" durch den Dateinamen der zu übertragenden Datei und den Login des Empfängers zu ersetzen, danach folgt *ohne Leerzeichen* "@rechnername:". rechnername ist dabei durch einen der im CIP stehenden Rechner zu ersetzen(siehe Benutzerhandbuch). Wenn Sie im CIP angemeldet sind, können Sie auch "@localhost:" benutzen. Der Empfänger muss dann nur noch sein Passwort eingeben und die Datei wird in sein Heimverzeichnis kopiert. Nach derselben Methode können Sie auch von zu hause Datein auf die CIP-Rechner kopieren, unter Angabe Ihres eigenen Logins als Empfänger. Der Doppelpunkt muss weiterhin bestehen. Nach dem Doppelpunkt können Sie einen alternativen Dateinamen eintragen oder ein Unterverzeichnis angeben.

2.3.3 USB-Sticks

Im CIP besteht die Möglichkeit, Daten auch per USB-Stick zu transferieren. Diese werden aber für alle Benutzer lesbar gemountet(d.h. in das Dateiverzeichnis eingeblendet). Versichern Sie sich deshalb mit dem Konsolenkommando

```
who
```

ob noch andere Benutzer an dem Rechner eingeloggt sind und arbeiten Sie nur kurz mit USB-Sticks. Für sensible Daten empfiehlt es sich, entweder der RBG das Kopieren zu überlassen, da die Rechner extra abgesichert sind oder einen anderen Weg der Datenübertragung zu wählen, zum Beispiel SSH/SCP.

2.3.4 Homepageordner

Früher wurden die Homepages durch Kopieren der zu veröffentlichen Dateien in das Verzeichnis public_html/und anschließendes Freigeben dieses Verzeichnisses veröffentlicht. Im Zuge der Umstrukturierung unserer Server ändert sich dieses Verfahren. Nun haben wir einen eigenen Homepageserver[4]. Dies erhöht die Sicherheit maßgeblich, weil wir so die internen Daten von den zu veröffentlichenden trennen können. Sie können Dateien entweder über den Webmailer Horde[5] oder mit SCP / SSH wie oben Beschrieben hochladen, der Servername ist *homepages.physik.uni-muenchen.de*.
Beachten Sie: *Dateien die auf diesem Server liegen können ohne Rechteveränderung von jedem anderen Benutzer gelesen werden*, der auch einen Account im CIP hat. *Der Passwortschutz durch den Webserver (durch .htpasswd-Dateien) ist aus diversen Gründen für Benutzer mit Account im CIP unwirksam.* Verlassen Sie sich also nicht auf diesen simplen Schutz und stellen Sie nicht allzu sensible Daten online.

[4] http://homepages.physik.uni-muenchen.de/~Benutzername

[5] https://webmail.physik.uni-muenchen.de , dann Mein Konto, Dateimanager, Web Homepage

2.4 Windows Terminal Server

Sie können sich auf einem Windowsserver durch Ausführen des Kommandos "win" einloggen. Bekanntermaßen sind Windowssysteme gerade beim surfen im Internet angreifbarer, da die Mehrzahl der Computernutzer Windows benutzt und sich daher auch die Schadsoftwareauthoren auf Windowssysteme konzentrieren. Surfen Sie daher besser unter Linux als dem Windowsterminalserver. Besuchen Sie nur bekannte Seiten und führen Sie nur bekannte Programme aus. Gehen Sie mit den Ressourcen schonend um, da alle Benutzer sich die Kapazität des Terminal Servers teilen.

2.5 Internetnutzung

Neben den Institutswebsites hat man im CIP auch Zugriff auf einen sehr schnellen Internetzugang. Dieser sollte vordergründig zu akademischen Zwecken genutzt werden. Besonders das Installieren von File-Sharingprogrammen oder ähnlichen, großen Datenverkehr verursachenden Programmen ist zu unterlassen. Das LRZ registriert eine steigende Anzahl von Missbrauchsfällen und ist eigentlich nicht gewollt, den Datenverkehr noch stärker zu filtern bzw. die Nutzung zu restriktieren. Zu diesem Punkt sei gesagt, dass der Datenverkehr generell Kosten verursacht, die auf die teilnehmenden Institutionen aufgeteilt werden. Darum sollte eine sachgemäße Nutzung selbstverständlich sein. Bemühen Sie sich, nicht ungewollt Spam oder anderen durch Schadprogramme verursachten Verkehr zu provozieren und die Grundregeln sicheren Surfens einzuhalten.

3 Abschließende Bemerkungen

Der Campusaccount war ein großer und effizienter Schritt zur Vereinheitlichung und Vereinfachung des Zugriffes für die Studierenden. Von Universitätsseite ist geplant, noch mehr Funktionen und Aufgaben über diesen Account und das Internet erreichbar zu machen. Ob dies auch verwirklicht wird, hängt auch davon ab, wie sicher die Accounts eingeschätzt werden.
Mit ein wenig Selbstdisziplin haben wir die Chance, viele Vorgänge von Studentenkanzlei bis zur Klausuranmeldung zu vereinheitlichen und abzukürzen.
Wir, die Rechnerbetriebsgruppe, halten es für sinnvoll, die zur Verfügung stehenden Kapazitäten und Rechenleistung allen Angehörigen der Fakultät für Physik möglichst frei zugänglich zu machen. Wir möchten auch in Zukunft nicht den Datenverkehr filtern oder Ausweiskontrollen durchführen. Sie als Benutzer des CIPs können durch Eigenverantwortung maßgeblich dazu beitragen, dass die Nutzung der PCs wie anderer Geräte weiterhin so unbeschränkt möglich ist wie bisher. Über Kritik oder Anregungen zu den angebotenen Diensten freuen wir uns immer.

Seien Sie auf der sicheren Seite, es lohnt sich.

Die Rechnerbetriebsgruppe der Fakultät für Physik