Sicherheit im Netz

Es ist allgemeine Erfahrung, dass es immer wieder zu unerlaubten Zugriffsversuchen auf Rechner kommt, die am Internet angeschlossen sind. Das gilt natürlich auch für die PCs im Universitätsbereich. Die Schäden, die Ihre PCs dabei erleiden können sind

- gelöschte oder veränderte Dateien
- Virusinfektionen
- gefälschte Mails
- Missbrauch Ihrer Daten

Zwei konzeptionelle Mängel im Internet führen zu diesen Sicherheitsproblemen:

1. Die unverschlüsselte Übertragung der Daten.
2. Die fehlende Sicherung von Authentizität und Integrität der Daten.

Ein großer Teil der von den Server-Administratoren des Rechenzentrums geleisteten Arbeit wird in die Verhinderung solcher Angriffe bzw. deren Folgen investiert.

Allgemeines

Passwörter und Login

Sie selbst können einen wichtigen Beitrag zur Verbesserung der Sicherheit im Internet leisten, wenn sie Ihre **Zugangsdaten geheimhalten**. Ihr personengebundenes (!) Passwort sollte dabei **folgende Kriterien** erfüllen:

- Verwenden Sie mindestens 8 Zeichen
- Setzen Sie keine Worte ein, die in Lexika enthalten sind oder mit Ihrem persönlichen Umfeld zu tun haben (Namen von Freunden oder Verwandten, Geburtsdaten usw.)
- Fügen Sie Sonderzeichen oder Ziffern ein. Manche Programme wehren sich allerdings z.B. gegen Fragezeichen; das Paragraphenzeichen sollten Sie auf dem PC meiden.
- Ändern Sie Ihr Passwort mindestens nach 6 Monaten.
- Schreiben Sie Ihr Passwort niemals auf und teilen Sie es niemandem mit.

Das Rechenzentrum gibt genaue Kriterien für die Passwörter vor, die Ihnen in https://myaccount.uni-freiburg.de auf den Passwort-Seiten bekanntgegeben werden.

Vergessen Sie nie, sich auch wieder abzumelden, wenn Sie an einem öffentlich zugänglichen Terminal eine Sitzung beenden, damit nicht nachfolgende Nutzer Ihren Zugang offen vorfinden. Besser noch, Sie schließen zusätzlich die verwendete Netzwerk-Anwendung (dies gilt besonders für die Web-Browser), damit nachfolgende Nutzer nicht durch einfaches Rückwärts-Navigieren Seiten angezeigt bekommen, die Sie zuvor besucht haben.

Verschlüsselung und digitale Unterschrift

Weiterhin haben sie die Möglichkeit, mit Hilfe zusätzlich installierter Software Ihre privaten Daten zu Verschlüsseln oder die lesbaren Daten mit einer digitalen Unterschrift zu versehen. Im ersten Fall kann man bei Verwendung eines Public Key Verfahrens erreichen, dass z.B. Ihre Mails nur von den Personen gelesen werden können, die dazu auch ermächtigt sind. Im zweiten Fall sind die Daten zwar für die Öffentlichkeit lesbar, können aber nicht unterwegs unbemerkt verfälscht werden. Ein weit verbreitetes Werkzeug für diesen Zweck ist Pretty Goot Privacy (PGP). Das Rechenzentrum bietet Ihnen über seine **Zertifizierungsstelle (Uni FR CA)** eine bequeme Möglichkeit, persönliche **Zertifikate** zu erwerben um sie für das Unterschreiben von Nachrichten zu verwenden.

Schutz des eigenen PC

Schützen Sie Ihren PC zu Hause mit einer Firewall-Software (wird z.B. bei Windows XP, Vista oder Windows 7 mitgeliefert) gegen mögliche Eindringlinge von außen, indem Sie möglichst viele Zugänge (Ports) schließen. Ein DSL-Router/Modem, bei dem die **NAT-Technik** zum Verbergen der internen Netzadressen verwendet wird, ist ein hervorragender Schutz gegen Angriffe aus dem Internet, macht aber auch Probleme bei einigen Kommunikationsverfahren.

Kommunikation

Die im Internet üblicherweise verwendeten Protokolle wie Telnet, Filetransfer (FTP), World Wide Web (WWW), Post Office (POP), Simple Mail Transfer (SMTP) usw. übertragen ihre Daten alle unverschlüsselt. Das gilt auch für die Loginphase der passwortgeschützten Zugänge, wie Telnet, FTP oder POP.

Angreifer, denen es gelingt, sich in den Datenstrom einzuklinken, sind in der Lage

- Benutzernamen und zugehörige Passworte im Klartext aufzuzeichnen,
- Daten mit einer fremden Identität zu versenden oder
- Daten in der Übertragungsphase unbemerkt zu manipulieren.

Aus diesem Grund gelten im Rechenzentrum schon seit einiger Zeit Einschränkungen bei den oben erwähnten Protokollen:

Alle passwortgeschützten Dienste wie Dialog, Filetransfer, Mail usw. sind nur über verschlüsselte Verbindungen zugänglich.
Beachten Sie bitte die folgenden Abschnitte zu diesem Thema.

Sensible Daten

Im Abschnitt „Verschlüsselung und digitale Unterschrift“ weiter oben wurde die Mail-Problematik bereits angesprochen.
Da die Übertragung einer E-Mail dem Transport einer Postkarte recht nahe kommt, was die Lesbarkeit für Unbefugte anbelangt, sollten Sie sich vor dem Versand sensibler Daten überlegen, ob Sie Ihre Mail

bzw. die Mail-Anhänge tatsächlich ohne Schutzmaßnahmen (s. oben) versenden wollen oder dürfen.

Wenn Sie Ihre Daten innerhalb einer geschlossenen Personengruppe teilen wollen, ist es durchaus überlegenswert, auf welchem Server Sie den Speicherbereich reservieren. Bei kommerziellen Speicher-Anbietern, die kleinere Bereiche eventuell auch kostenlos zur Verfügung stellen (Stichwort: Cloud), haben Sie in der Regel keine Informationen darüber, wer ggf. zusätzlich Zugriff auf Ihre Daten bekommen kann. Wesentlich transparenter ist dagegen die Situation, wenn Sie die Daten z.B. auf einem Speicherbereich des Rechenzentrums oder des eigenen Instituts Ihrer Heimat-Universität hinterlegen.
Die Ideale Situation ist in der Cloud dann gegeben, wenn Sie über ein geeignetes, lokal installiertes Programm die Daten **vor dem Upload** auf unbekannte Server verschlüsseln und erst **nach dem Download** wieder entschlüsseln können. Ein Beispiel dafür ist der Cloud-Speicher **Wuala**.

Secure Shell (SSH)

Secure Shell (SSH) ist ein Verfahren, das die Dialogprotokolle Telnet, rsh (remote shell), rlogin (remote login) und rcp (remote copy) frei von den oben genannten Mängeln ersetzen soll. Dabei wird in der Einleitungsphase das sog. Public Key Verfahren angewendet, bei dem ein öffentlicher Schlüssel zum Verschlüsseln und ein dazugehöriger geheimer (privater) Schlüssel zum Entschlüsseln verwendet wird. Während dieser sehr gut abgesicherten Phase handeln die Kommunikationspartner einen gemeinsamen (symmetrischen) Schlüssel für die spätere Datenübertragungsphase aus, der nur für diese Sitzung oder einen Teil davon gilt.

Sie führen also mit einem auf Ihrem PC installierten SSH-Client Dialogsitzungen auf entfernten Rechnern durch, wie Sie es z.B. mit Telnet bisher gewöhnt waren. Ein hierfür geeignetes Programm wird im folgenden Abschnitt zum Download angeboten. Daneben finden Sie dort auch einen Verweis auf die Installationsanleitung.

Die Anmeldung geht prinzipiell in folgenden Schritten vonstatten:

1. Das Client-Programm baut die TCP/IP-Verbindung zum Server auf. Standard-Port: 22
2. Aushandeln der Protokoll-Versionen.
3. Der Server sendet zwei öffentliche RSA-Schlüssel (Public Host Key und Public Server Key) und die unterstützten symmetrischen Verschlüsselungsverfahren.
4. Der Client verifiziert den Public Host Key des Servers.
5. Der Client generiert zufällig einen Session-Key, verschlüsselt ihn mit den beiden RSA-Keys und sendet ihn zusammen mit dem ausgewählten symmetrischen Verfahren an den Server.
   Ab jetzt läuft die Kommunikation verschlüsselt ab.
6. Der Client authentifiziert sich (s. nächste Liste!).
7. Die Benutzerumgebung wird bereitgestellt und der Austausch der Nutzerdaten beginnt, wobei eine symmetrische Verschlüsselung mit dem zuvor ausgetauschten Sitzungsschlüssel verwendet wird.

Die Authentifizierung des Client kann auf verschiedene Arten erfolgen. Die beiden wichtigsten sind:

- **Authentifizierung über das Kennwort** (Password) des Benutzers.
  Die Übermittlung erfolgt bereits verschlüsselt. Diese Methode ist für die PC-Benutzer am einfachsten zu realisieren und wird von uns empfohlen.

- **Authentifizierung über RSA-Schlüssel.**
  Hier weist der Client die Kenntnis des privaten Schlüssels nach. Dazu muss der öffentliche Schlüssel des Benutzers beim Server hinterlegt werden. Der private Schlüssel des Client muß gegen Zugriff anderer unbedingt geschützt werden. Dazu dient die Passphrase, die als Kennwort für die Verschlüsselung des RSA-Schlüsselpaares verwendet wird. Falls Sie mehrere Verbindungen mit unterschiedlichen Schlüsseln verwalten, können Sie durch die einmalige Angabe der Passphrase beim Start des Kommunikationsprogrammes den Zugriff auf alle Schlüssel öffnen, so lange die Anwendung läuft. Weitere Passwortangaben sind in dieser Zeit dann nicht mehr nötig.

Ein wichtiger Begriff im Zusammenhang mit SSH-Anwendungen ist das **Port Forwarding**.

Man versteht darunter die Fähigkeit der SSH-Verbindung, die Daten anderer Internet-Dienste wie FTP, X11, POP oder HTTP durch die verschlüsselte Strecke zu „tunneln“. Dadurch profitieren diese unsicheren Protokolle vom Verschlüsselungsmechanismus der SSH-Verbindung und können auch dann weiter verwendet werden, wenn die unverschlüsselten Zugänge geschlossen sind. Diesen Vorteil erkauft man sich allerdings mit einer umständlicheren Handhabung: Bevor Sie die unverschlüsselte Verbindung eröffnen können, müssen Sie zuvor natürlich eine SSH-Verbindung zum entsprechenden Rechner aufgebaut haben. Außerdem müssen Sie Änderungen an der Konfiguration der nicht verschlüsselnden Clients vornehmen. Bei **FTP** kommt noch hinzu, daß der Client in der Lage sein muß, die Sitzung **im passiven Modus** (PASV-Mode) zu betreiben.

Das unten angebotene Produkt SSH2 macht mit Hilfe seiner Komponente **Secure FTP** die Tunnelung eines üblichen FTP-Programmes überflüssig. Stattdessen wird über ein gesondertes, äußerst flexibles Datei-Explorer-Fenster die in **SSL Version 2** enthaltene Dateiübertragungsmethode zur Verfügung gestellt.

Secure Socket Layer (SSL)

Secure Socket Layer ist ein von Netscape entwickeltes Verfahren, um Daten über verschlüsselte Strecken zu transportieren. Dieser Standard erfordert kein benutzerseitiges Kennwort. Lediglich der Server identifiziert sich dem Benutzer gegenüber mit Hilfe eines **digitalen Zertifikates**. Sobald der Benutzer das Zertifikat des Servers akzeptiert, wird eine verschlüsselte Verbindung aufgebaut.

Alle modernen Webclients verwenden heutzutage die Verschlüsselungsmethode **SSL** (dabei kommt das Protokoll HTTPS zum Einsatz) und können im obigen Sinne als sicher eingestuft werden.

Eine schöne, leicht verständliche Übersicht über den Aufbau einer SSL-Verbindung wird vom Oberstufenzentrum Handel in Berlin ins Netz gestellt:
http://oszhdl.be.schule.de/gymnasium/faecher/informatik/krypto/ssl-verbindungsaufnahme.pdf

Das Produkt stunnel (SSL-Tunnel) für 32-bit Windows (95/98/XP) erlaubt die Errichtung von port forwarding - Strecken mit Hilfe des SSL-Verfahrens. Wenn Sie z.B. nicht auf ein Kommunikationsprogramm verzichten können oder wollen, das von sich aus keine verschlüsselte Verbindung unterstützt, ist der Einsatz von Stunnel die Methode der Wahl, sich eine solche zu verschaffen.

Da die meisten Kommunikationsprogramme heutzutage SSL beherrschen, handelt es sich beim stunnel um eine aussterbende Technik.

Download

	**Download** und Installation des Software-Paketes SSH2.
	**Download und Installation** des Softwarepaketes STUNNEL

Sicherheit - Artikelübersicht, Netz - Artikelübersicht, Zertifikate - Artikelübersicht