Freie Universität Berlin

{tip4u://020} Version 5

Zentraleinrichtung für Datenverarbeitung (ZEDAT)
www.zedat.fu-berlin.de

Sicherheit von E-Mail

In diesem Tip4U finden Sie Hinweise zur sicheren Kommunikation per E-Mail.

zedat

Zentraleinrichtung für Datenverarbeitung
Fabeckstraße 32 / 14195 Berlin
Hotline (030) 838 77777 / hilfe@zedat.fu-berlin.de

Sicherheit von E-Mail

E-Mail ist ein sehr zuverlässiges, schnelles und bequemes Kommunikationsmedium. Per E-Mail kann man mit Korrespondenzpartnern nicht nur kurze Textnotizen, sondern auch Dateien verschiedener Formate und beliebigen Inhalts austauschen, sofern gewisse Größen nicht überschritten werden. Jedoch müssen beim Umgang mit diesem Medium verschiedene Aspekte berücksichtigt werden. Besondere Beachtung verdient die Frage nach der Sicherheit von E-Mail, deren verschiedene Facetten im Folgenden kurz erläutert werden:

Vertraulichkeit

E-Mails werden in der Regel nicht auf direktem Wege vom Absender zum Empfänger über das lokale Netz bzw. das Internet transportiert. Meist durchläuft eine E-Mail auf ihrem Weg viele Stationen (sprich: Mailserver), die der Absender weder vorhersehen noch beeinflussen kann. Jedem Administrator eines beteiligten Mailservers ist es im Prinzip möglich, eine E-Mail auf ihrem Weg „abzufangen“ und vor ihrem Weitertransport einzusehen. In der Praxis kommt dies jedoch kaum vor. E-Mail verhält sich insofern wie eine Postkarte.

Will man jedoch sicher sein, dass eine E-Mail mit vertraulichem Inhalt ausschließlich vom Empfänger gelesen werden kann, muss man sie vor dem Versand verschlüsseln. Stichworte hierzu sind u. a. PGP und GnuPP - letzteres ist als eine vom Bundesministerium für Wirtschaft und Technologie geförderte Software kostenlos erhältlich.

Authentizität und Integrität

Jede E-Mail trägt in einer Kopfzeile (Header) Angaben zum Absender. Wie bei der gelben Post sind diese Angaben sehr leicht fälschbar, also unzuverlässig. Soll der Empfänger einer E-Mail sicher sein, dass der vorgebliche Absender auch tatsächlich der Versender einer E-Mail ist, muss die E-Mail vom Absender signiert werden. Hier werden ähnliche Verfahren angewandt wie bei der Verschlüsselung. Die E-Mail bleibt hierbei unverschlüsselt, erhält aber eine Art Stempel oder Wasserzeichen als Echtheitsmerkmal. Eine Signatur garantiert zugleich auch die Unversehrtheit einer E-Mail, verhindert also eine unbeabsichtigte oder vorsätzliche Veränderung auf dem Transportweg. Signaturen und Verschlüsselung werden häufig miteinander kombiniert.

Schutz personenbezogener Daten

Die Verarbeitung und Übermittlung personenbezogener Daten - dazu gehört insbesondere der Versand per E-Mail - unterliegt den besonderen Bestimmungen einschlägiger Datenschutzgesetze und -verordnungen. Die Verarbeitung personenbezogener Daten ist auf den Systemen der ZEDAT nur nach Genehmigung der ZEDAT zulässig. Eine entsprechende Klausel akzeptiert jeder Nutzer der ZEDAT mit dem Antrag auf eine Benutzungsberechtigung (Account-Antrag).

Sichere Ablage von E-Mails

E-Mails werden nicht nur geschrieben, versandt oder gelesen, sondern auch als Dateien auf Rechnern gespeichert. Dies gilt sowohl für selbst verfasste und versandte (Kopie bleibt

beim Absender) als auch für empfangene E-Mails (Ablage). In beiden Fällen muss man unterscheiden, ob sich gespeicherte E-Mails auf einem zentralen Server, z. B. dem Mailserver der ZEDAT, oder auf einem lokalen Arbeitsplatzrechner (PC) befinden. Auf einem zentralen Server sind die E-Mails vor fremdem Zugriff sicher - vorausgesetzt, das Passwort ist nur dem Account-Inhaber bekannt.

Befinden sich abgelegte E-Mails jedoch auf einem PC, gelten hier ausschließlich die lokal festgelegten Zugriffsbeschränkungen. Nur Betriebssysteme, die eine lokale Account-Verwaltung mit Passwortschutz zulassen, können ein Mindestmaß an Vertraulichkeit gewährleisten. Auch in diesem Fall gilt: Das Passwort darf nur dem Inhaber bekannt sein und nicht an Dritte weitergegeben werden. Jedoch kann jeder, der physischen Zugang zu einem PC hat, mit einem gewissen Aufwand den Passwortschutz umgehen und sämtliche Dateien des Rechners auslesen.

Sicherheit von Webmail

Eine Möglichkeit des Zugriffs auf zentral gespeicherte E-Mails auf dem ZEDAT-Mailserver bietet das ZEDAT-Portal mit der Funktion Webmail. Hierbei können mit einem Web-Browser sowohl E-Mails verfasst und versendet als auch archiviert und organisiert werden (Ablage). Der Datenverkehr zwischen dem PC und den Servern erfolgt dabei verschlüsselt und ist somit vor dem „Ablauschen“ durch Dritte geschützt.

Wegen vermeintlicher Bequemlichkeit nutzen jedoch einige Anwender auch das Angebot von Firmen, E-Mails mittels Webmail zu versenden und zu empfangen. Manche dieser Anbieter gestatten es, E-Mails automatisch von einem ZEDAT-Account abzuholen und auf den Server des Dienstleisters zu übertragen. Hierzu ist es erforderlich, das ZEDAT-Passwort dem fremden Server mitzuteilen. Da weder Sie noch die ZEDAT die Zuverlässigkeit und Vertrauenswürdigkeit eines solchen Anbieters prüfen oder gewährleisten können, ist von der Nutzung entsprechender Dienste dringend abzuraten. Die Nutzung fremder Anbieter für E-Mails mit vertraulichen Inhalten verbietet sich aus demselben Grunde.

Sicherheit vor Viren

Eine besondere Gefahr für die Sicherheit von E-Mail bilden Viren, die sich per E-Mail oder auf anderem Wege in einen Rechner einschleichen. Viren können nicht nur einen Rechner unbrauchbar machen, manche versenden selbstständig Dateien von ihrem Wirtsrechner an beliebige E-Mail-Adressen. Darunter können sich natürlich insbesondere auch vertrauliche Inhalte befinden.

Besonders gefährdet sind - im Gegensatz zu zentralen Mail-Servern - Arbeitsplatz-PCs. Einen wirkungsvollen Schutz vor Viren bietet nur der Einsatz stets aktuell gehaltener Software (Betriebssystem, Web-Browser, E-Mail-Programm) sowie eines aktuellen Anti-Viren-Programms, das zudem kontinuierlich mit den neuesten Viren-Informationen versorgt werden muss.

Spam und die Vertraulichkeit von E-Mail-Adressen

Ein Aspekt, der Datenschutz und Netiquette gleichermaßen berührt, ist die Vertraulichkeit von E-Mail-Adressen. Soll eine E-Mail an eine größere Zahl von Empfängern verschickt werden, gebieten es Höflichkeit und Datenschutz, die Adressen aller Empfänger nicht in

die Anschriftenfelder „To:“ („An:“) oder „Cc:“ („Kopie an:“) zu schreiben. Dort kann nämlich jeder Empfänger die Adressen sämtlicher anderer Empfänger lesen. Nur in seltenen Fällen wird dies ausdrücklich erwünscht sein. Besser ist es, die Adressaten einer solchen Rundmail in das „Bcc:“-Adressfeld zu schreiben. Dort bleiben Zahl und Details der Adressaten vor den Augen der Empfänger verborgen. In jedem Fall muss vor dem Versand von Rundmails geprüft werden, ob es sich nicht um Spam handelt, also den unerbetenen Versand von E-Mails größerer Zahl an fremde Empfänger. Jeder E-Mail-Nutzer kennt aus eigener leidvoller Erfahrung das Phänomen einer mit Werbung oder Schlimmerem verstopften Mailbox.