Universität Zürich
Informatikdienste

Sicherheitsempfehlungen für Informatikanwender (SIA)

Diese Sicherheitsempfehlungen für Informatik-Endbenutzer sind sowohl anwendbar auf mobile und Arbeitsplatzgeräte im Besitz der Universität wie auch auf mobilen Geräten im Privatbesitz bzw. von Lieferanten, welche am Netzwerk der Universität tätig sind.

Diese Empfehlungen dienen als einfache Checkliste, um einen minimalen Sicherheitsstandard auf den lokalen Arbeitsplatzgeräten zu gewährleisten. Es ist wichtig, dass die einzelnen Punkte regelmässig und vor allem auch nach längeren Abwesenheiten (z.B. Ferien) durch den Systemnutzer überprüft werden.

Informatik-Betreuer

In vielen Fällen werden Sie nicht die Administrationsberechtigungen haben, um Systemaktualisierungen („Patches“) selbst einzuspielen. Daher ist es wichtig, dass Sie Ihren Informatik-Betreuer kennen und ihn zur Systemaktualisierung ermutigen und dabei unterstützen.

Empfehlung:

- Stellen Sie sicher, dass Sie ihren Informatik-Betreuer und seinen Stellvertreter kennen und sprechen Sie mit ihm über Informatik-Sicherheit. Die entsprechende Koordinatorenliste finden Sie unter http://www.id.unizh.ch/services/koord/.
- Aktuelle Bedrohungen und Massnahmen werden jeweils auf der Homepage der Universität Zürich publiziert (http://www.unizh.ch). Besuchen Sie diese Seite regelmässig, v.a. aber, wenn Sie ein Ereignis vermuten.

Umgang mit dem Internet

Das Herunterladen von Software, Musik und Filmen und anderen Daten von Quellen im Internet kann die Integrität Ihres Systems gefährden. Viren und Würmer können sich schnell einmal in harmlos erscheinenden Dateien verstecken. Sollte die Quelle zudem nicht Eigentümer der Rechte an den geladenen Daten sein, so verletzen Sie das Urheberrecht.

Empfehlung:

- Laden Sie nur Daten von Internet-Quellen, denen Sie absolut vertrauen.
- Stellen Sie keine Musik, Filme oder Software im Internet zur Verfügung, für welche Sie nicht über die Urheberrechte verfügen.
- Installieren und nutzen Sie keine Software für elektronische Tauschbörsen (z.B. Kazaa, eDonkey). Diese Programme können ohne Ihr Wissen dem Internet Daten von Ihrer Festplatte zur Verfügung stellen (inkl. Filme, Musik).

Umgang mit E-Mail

Verschiedene Viren und Würmer, welche sich heute verbreiten, verstecken sich in E-Mail-Anhängen. Vermeiden Sie es daher grundsätzlich, solche Anhänge zu öffnen, ausser Sie kennen den Absender der E-Mail, die E-Mail ist an Sie persönlich adressiert oder Sie haben die E-Mail erwartet. Aber Achtung: Sowohl Absender- wie Empfängeradresse können gefälscht sein !

Empfehlung: Fragen Sie den Absender im Zweifelsfall an, ob er Ihnen bewusst diese E-Mail geschickt hat. Sollte die Antwort negativ sein, so handelt es sich mit grosser Wahrscheinlichkeit um ein Virus.

Aktualisierung des lokalen Virenschutzes

Für die Installation des lokalen Virenschutzes ist in der Regel der Informatik-Koordinator zuständig. Moderne Software kann so eingerichtet werden, dass sie sich automatisch aktualisiert. Dennoch kann es vorkommen, dass diese Aktualisierung nicht (mehr) korrekt funktioniert.

Empfehlung:

- Informieren Sie sich bei Ihrem Informatik-Koordinator, wie Sie den Aktualitätsstand des Virenschutzes persönlich überprüfen können.
- Sobald Sie das Verfahren kennen, prüfen Sie den Zustand regelmässig.
- Stündliche oder mindestens tägliche automatische Aktualisierungen sind empfohlen.

Physische Sicherheit

Gefahren drohen auch bei physischem Zugriff auf Ihr System.

Empfehlung:

- Falls Sie ein Einzelbüro besitzen, so schliessen Sie es bei längerer Abwesenheit während des Tages ab.
- In jedem Fall blockieren Sie den Zugriff mit dem im Betriebssystem eingebauten Zugangsschutz. Dieser kann auch so eingerichtet werden, dass er bei längerer Inaktivität automatisch aktiviert wird.
- Melden Sie sich am Ende des Tages am System ab.
- Falls Sie ein Notebook benutzen, schliessen Sie es ein.

Profile und Passwörter

Die meisten Betriebssysteme erlauben das Einrichten und Verwalten von Passwort-geschützten Benutzerprofilen. Diese Profile sind mit unterschiedlichen Rechten versehen und daher auch mehr oder weniger anfällig auf Virenbefall.

Empfehlung:

- Wählen Sie Passwörter, welche aus Buchstaben, Zahlen und Sonderzeichen zusammengesetzt sind und aus mindestens 8 Zeichen bestehen.
- Verwenden Sie keine Benutzerkonti, welche von mehreren Personen genutzt werden bzw. teilen Sie Ihre Passwörter niemandem mit.
- Sollten Sie über ein Administrator-Konto verfügen, vergessen Sie nicht, auch dieses mit einem sicheren Passwort zu versehen.
- Stellen Sie Ihr Profil so ein, dass die Dateieendungen sichtbar sind und seien Sie skeptisch, wenn Sie unbekannte, ausführbare Dateien (.exe) in Ihren Verzeichnissen finden.
- Geben Sie Ihre Passwörter nicht in Webformulare ein, welche Sie nicht kennen.

Persönliche Firewalls

„Firewalls“ sind Hard- oder Softwarekomponenten, welche ein System oder ein Netzwerk vor unerlaubtem Zugriff über das Datennetz schützen sollen. Dies ist dann besonders wichtig, wenn Ihr System abgeschaltet, längere Zeit vom Netzwerk getrennt oder an einem anderen Netzwerk angeschlossen war (z.B. bei einem privaten Provider). In diesen Fällen schützt eine richtig konfigurierte Firewall Ihr System, bis es wieder mit den neusten Systemaktualisierungen und Virenbeschreibungen bestückt ist.

Persönliche Firewalls werden auf dem lokalen Arbeitsplatzgerät installiert und müssen entsprechend konfiguriert und regelmässig aktualisiert werden.

Empfehlung: Besprechen Sie dieses Thema mit Ihrem Informatik-Betreuer. Er wird gemeinsam mit Ihnen entscheiden können, ob es für Sie sinnvoll ist, eine persönliche Firewall zu betreiben.

Bei weiter gehenden Fragen wenden Sie sich bitte per E-Mail an die Spezialisten der Informatikdienste unter security@id.unizh.ch.