ISPConfig

- Adminoberfläche von ISPConfig auf https gesicherte Verbindung umstellen

Adminoberfläche von ISPConfig auf https gesicherte Verbindung umstellen

> Veraltet: Inzwischen kann direkt bei der Installation von ISPConfig die https-Verschlüsselung aktiviert werden.

Diese Anleitung wurde mit ISPConfig 3.0.1.3 auf einem CentOS 5.3 getestet.

Standardmäßig läuft die Adminoberfläche von ISPConfig unverschlüsselt auf Port 8080. Da darüber aber etwa auch neue Benutzer angelegt, Mailboxen und Datenbanken konfiguriert werden, empfiehlt es sich schon das auf eine SSL-gesicherte Verbindung umzustellen.

Dazu muss nur die Konfigurationsdatei für den ISPConfig-Vhost angepasst werden, das dafür nötige SSL-Zertifikat habe ich inkl. Key unter /etc/pki/tls/certs -/key abgelegt.

Hier die Ergänzungen für die Konfigurationsdatei:

/etc/httpd/conf/sites-available/ispconfig.vhost

```
  <IfModule mod_ssl.c>
    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/meinserver.de.crt
    SSLCertificateKeyFile /etc/pki/tls/private/meinserver.de.key
  </IfModule>
```

Die gesamte Datei sieht jetzt folgendermaßen aus:

/etc/httpd/conf/sites-available/ispconfig.vhost

```
###########################################################
# This virtual host contains the configuration
# for the ISPConfig controlpanel
###########################################################

Listen 8080
NameVirtualHost *:8080

<VirtualHost _default_:8080>
  ServerAdmin webmaster@localhost

  <IfModule mod_fcgid.c>
    DocumentRoot /var/www/ispconfig/
    SuexecUserGroup ispconfig ispconfig
    <Directory /var/www/ispconfig/>
      Options Indexes FollowSymLinks MultiViews +ExecCGI
      AllowOverride AuthConfig Indexes Limit Options FileInfo
      AddHandler fcgid-script .php
      FCGIWrapper /var/www/php-fcgi-scripts/ispconfig/.php-fcgi-starter .php
      Order allow,deny
      Allow from all
    </Directory>
  </IfModule>

  <IfModule mod_php5.c>
    DocumentRoot /usr/local/ispconfig/interface/web/
    AddType application/x-httpd-php .php
```

```
    <Directory /usr/local/ispconfig/interface/web>
      Options FollowSymLinks
      AllowOverride None
      Order allow,deny
      Allow from all
          php_value magic_quotes_gpc        0
    </Directory>
  </IfModule>

  <IfModule mod_ssl.c>
    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/meinserver.de.crt
    SSLCertificateKeyFile /etc/pki/tls/private/meinserver.de.key
  </IfModule>

  # ErrorLog /var/log/apache2/error.log
  # CustomLog /var/log/apache2/access.log combined
  ServerSignature Off

</VirtualHost>

<Directory /var/www/php-cgi-scripts>
    AllowOverride None
    Order Deny,Allow
    Deny from all
</Directory>

<Directory /var/www/php-fcgi-scripts>
    AllowOverride None
    Order Deny,Allow
    Deny from all
</Directory>
```

Wenn man verhindern will, dass die Verbindung auf keinen Fall unverschlüsselt erfolgt, entfernt man die beiden folgenden Zeilen aus der Konfiguration:

```
  <IfModule mod_ssl.c>
    ...
  </IfModule>
```

Apache würde damit beim Starten mit einem Fehler abbrechen wenn mod_ssl nicht installiert ist.