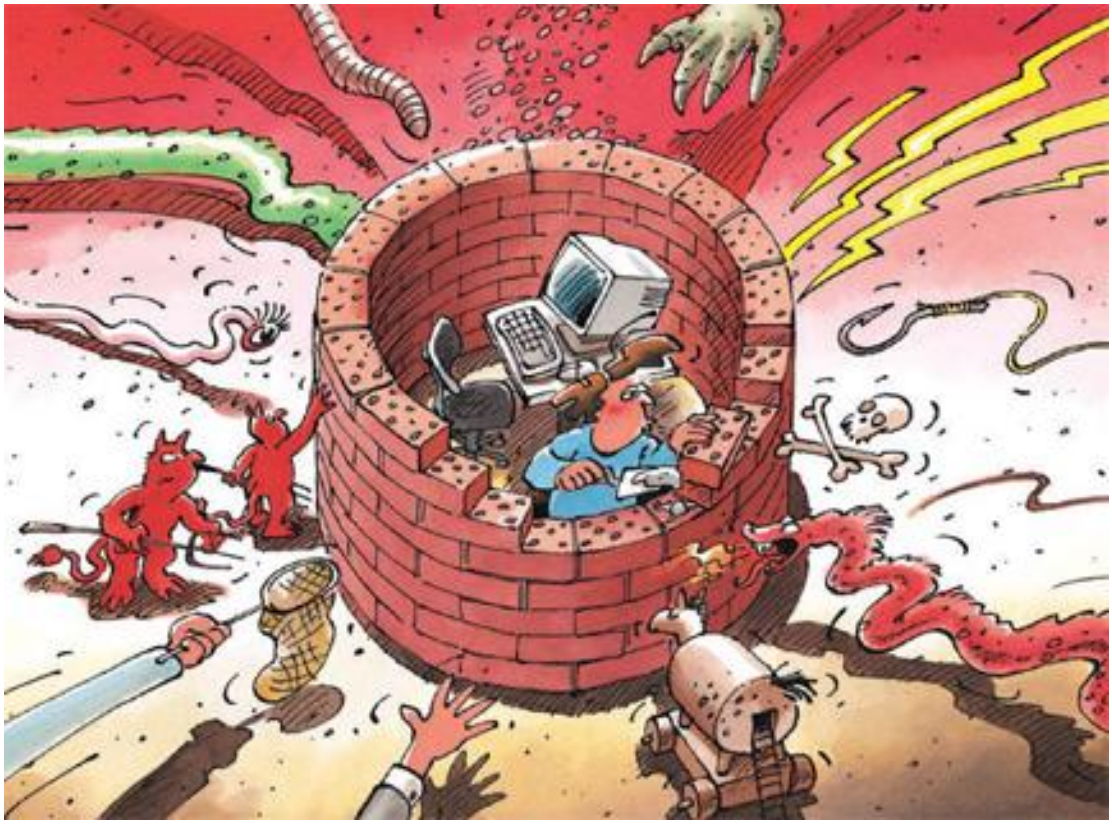
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

Reporting and Analysis Centre for Information Assurance MELANI
www.melani.admin.ch

Security Measures for Content Management Systems (CMS)

29. october 2013



1 Introduction

The number of websites has truly exploded over the past few years. This is in part because even users without technical expertise can often place their own website on the Internet with easy-to-use tools and at lower and lower costs. Content management systems (CMSs) are often used for this purpose, with which a website can be designed and placed online with only a few clicks and without detailed knowledge in web design. There are now dozens of such CMSs used by hobby website operators, SMEs, and others. The increasing popularity of these systems makes them interesting for cybercriminals as well, who invest all the more energy and effort in their search for vulnerabilities the more popular a software program is and accordingly the greater the number of potential targets. Not only CMSs, but every software program has potential vulnerabilities – no program is guaranteed to be secure. Moreover, software developers implement new functions all the time. But with each additional line of code, the software not only gets more functions, but its complexity also increases and accordingly the risk that it might have a vulnerability somewhere.

Attacks on CMSs can be reduced dramatically by way of *patching* (prompt incorporation of security updates). However, several other measures can contribute to the security of CMSs.

2 Summary

Detailed instructions can be found further down in this document. .

7 Measures to secure Content Management Systems

1. Prompt incorporation of security updates
2. Two-factor authentication
3. Restriction of administrator access to certain IP addresses
4. Restriction of administrator access using a .htaccess file
5. Securing the computer of the webmaster
6. Web application firewall
7. Early recognition of vulnerabilities.

3 Security Measures for Content Management Systems

There are several measures that contribute to the security of CMSs:

1. **Prompt incorporation of security updates**
   A security patch has to be implemented immediately, once it appears.

2. **Two-factor authentication**
   Besides the normal authentication (username and password) which is needed to access the administration area of a CMS, MELANI recommends the use of a two-factor authentication. Such an additional one time password (OTP) can be generated for example with the software Google Authenticator. It installs an app on your Mobile Phone (Android, iOS, Blackpberry), which generates every 60 seconds a new OTP. Google Authenticator can be installed on the webserver (CMS) with an appropriate plug-in, which already exists for numerous different Content Management Systems like Wordpress or Typo3.

3. **Restriction of administrator access to certain IP addresses**
   Such a restriction can be extended to IP-address, IP-range or on the geolocation of an IP-address. Such plugins already exist for a number of Content Management Systems.

4. **Restriction of administrator access using a .htaccess file**
   The advantage of this measure is that it not only restricts the IP-range, but it is also possible to implement an additional authentication, such as (Username / Password) (Basic Authentication).

5. **Securing the computer of the webmaster**
   It is often the case that websites and CMS are being compromised through stolen FTP credentials. Normally, this is done by means of a Trojan on the webmaster's computer. It is therefore imperative that the webmaster makes sure that the computer he is using is not only free from malware, but also is also protected by an up-to-date antivirus software. In addition, the FTP-connections (sFTP) should be encrypted if possible.

6. **Web Application Firewall.**
   With an Web Application Firewall (WAF) it is possible to block attacks before they reach the application. There are many different WAF-solutions. The most famous open-source solution is ModSecurity.

7. **Early recognition of vulnerabilities.**
   The ultimate goal is to be able to identify potential security gaps before the criminals do. Here too, there are many different solutions to be found on the Internet. Some of which are even free.