You should enable only those services, which your web application needs. Otherwise, you provide more opportunities for attackers to infiltrate your system. Many services are installed by default, so you should take care to disable those you do not actually need.

Server security

If you run your web applications locally on your own servers, then you should check which services run on your server and IIS. Then turn off everything your web application does not need. You should also patch your operating system and server regularly. When a serious security issue is announced, you should patch your system as soon as possible, because the attackers are usually able to exploit the flaws within 24 hours.

If your web applications run on remote servers (webhosting, cloud, etc.), all you can do is trust your provider to ensure the server security.

Kentico security

We recommend that you install only necessary modules (or that you uninstall unused modules after the installation). You can choose which modules will be installed with Kentico in the Custom installation, and you can also add or remove modules and components after the installation – see Adding and removing components from an installed Kentico web project.

You should also restrict public access to unused files located in */CMSPages* and */CMSModules/<some module>/CMSPages* directories. The following example restricts the public access for the GetCMSVersion.aspx page:

```
<location path="CMSPages/GetCMSVersion.aspx">
    <system.webServer>
        <security>
            <authorization>
                <remove users="public" roles="" verbs="" />
                <add accessType="Allow" users="*" roles=""/>
            </authorization>
        </security>
    </system.webServer>
</location>
```

Hotfixing

We recommend installing hotfixes only when you need them – in cases when the hotfix repairs bugs that are causing you problems. You can install hotfixes using KIM or download them from Kentico portal.

You should also know that we do not publicly announce our security issues. If we did, we would make it easier for the attackers to determine the issue and attack servers, that are not updated yet.

If you desire to be informed about security issues in Kentico, sign up to our security newsletter on the client portal (this newsletter is available only if you have prepaid maintenance service).