Imagine that you’re running a largish online service. What actions would you need to take to secure your service? Please elaborate on both the action and the reason for it. Try to find at least 7 actions.

When running an online service there are best practices that need to be followed in order to guarantee that the service itself is secure. There are several points of the service that need to be secured and protected from malicious use.

There are several weaknesses that are inherent to a service, for that reason the points of interest have to follow some set of guidelines in order to be secure. For instance, a point of interest can be the data, the operating system or the infrastructure itself.

In order to secure the data, there are two parts to it. The security of the data and the protection of data while in transit, the integrity of the data so to speak.

The security of the data is generally guaranteed by some kind of encryption of the data, be it sever-sided or not. To further protect data that is stored in the online service there are a number of actions that can be performed. You may want to add these to the service as there are possible threats to the data such as accidental data deletion, compromise of data integrity through modification or most notably information disclosure of confidential information that can be accessed through the service. To prevent these things from occurring you may want to add a permission system to limit access to confidential files, or a backup system to enabling recovery of deleted files. Other ways of securing and saving data are versioning and replication. Server-side and or client-side encryption of data is also recommended to ensure the security of the data.

When it comes to protecting data that is in transit accidental information disclosure and the compromise of data integrity are also possible threats, but additionally spoofing or man-in-the-middle attacks pose an additional form of threats. To mitigate these threats traffic should occur on at least a HTTPS connection or even a SSH connection.

As already mentioned there is also the need to secure the own operating system and application as well as the infrastructure. The infrastructure should be resistant to threats such as denial of service attacks or any form of flooding.