Table of Contents

Hardening Guide: Ensuring Server Security 1
1. Never Leave Devices Unattended 1
2. Server Password Security 1
3. Set Up Access Limitations to Your Computers Files 1

BioStar 2, Server, Security, Hardening

Hardening Guide: Ensuring Server Security

Servers hold confidential organizational data and information. An insecure server is vulnerable to all sorts of security threats and data breaches. Security vulnerabilities can lead to the loss of critical data or loss of control and capability that can jeopardize the whole organization.

To protect your BioStar 2 server and the information it contains, make sure that the server itself is physically secure and the access to the operating system, especially administrator access, is carefully controlled. Once a malicious actor gains physical and/or logical access (including via remote) to a server, there are many ways to compromise the system by modifying settings in BioStar 2 directly or by accessing and modifying the database, obtaining encryption keys and more.

Below are three points which are common, but often neglected:

1. Never Leave Devices Unattended

The physical security of your devices is just as important as their technical security.
- If you need to leave the device, lock it up so no one else can use it: the screen and the room.
- Make sure the server room is protected, either from human or environmental factors. This can be achieved by controlling the access to the room, installing alarm and monitoring system, and regularly conduct building security assessments.

2. Server Password Security

When it comes to server security, make sure to use password best practices. The first step is to develop clear cut password policies and rules that all personnel should follow.
- Enforce minimum character length for passwords, set password complexity guidelines, enable session timeout for inactivity, and use a multiple-factor authentication strategy.
- Set password expiration policy. Passwords should only last a few weeks or months. Encourage all users to implement safe password storage to avoid passwords landing in unsafe hands.
- The most important is the administrator account. Any program on a server can be compromised if the administrator access is obtained. Make sure to strictly follow the account’s password guidelines and who should this access be given to.

3. Set Up Access Limitations to Your Computers Files

Allowing access to the server either directly or remotely can allow unauthorized person to compromise certain areas of the system. That is why most operating systems have the option to specify access privileges. It is best to be as restrictive as possible for server safety.
- Specify access privileges to directories, networks, files, and other server elements. Access controls can reduce both deliberate and unintended server security breaches.

- Limiting read access can protect confidential and classified information. Similarly, restricting who can modify files and data will help to enforce the integrity of the files.
- Not all employees should be given access to the organization’s resources. Applying the principle of the least privilege (a subject should be given only those privileges needed for it to complete its task) is an excellent move in securing servers.
- People who have no business with server resources or do not need them to fulfill their job requirements should not have access to those resources.