What is a hardened server?

The server hardening process reduces your business' attack surface and helps you guard against ransomware, malware, and other cyberthreats. You can follow this process to protect all points of entry against cyberattacks, address cybersecurity weaknesses, and optimize your security posture.

About Server Hardening

A server is a computer program or device that supports another program and its end-user (client). It is part of a client/server model in which a server program receives and fulfills requests from client programs.

Servers consist of physical or virtual machines or software. A physical server is used to run software. Comparatively, a virtual server operates like its physical counterpart but does not require any physical components. Meanwhile, a software-based server consists of an operating system and application. Together, these components provide access to hardware and services that the application needs to run.

The National Institute of Standards and Technology (NIST) defines "hardening" as a process used to patch vulnerabilities or turn off non-essential services.

With hardening, your business can eliminate cybercrime attack vectors and unnecessary server processes.

For example, your company can "harden" access to certain system applications, ports, or user accounts. This removes potential vectors a cybercriminal can use to attack your company.

What Is an Attack Surface?

An attack surface refers to any entry points that a cybercriminal can use to infiltrate your company's servers. It consists of your network interfaces, software, and applications. Your attack surface can grow or shrink, depending on how you manage your systems.

If your company adds systems, it increases its attack surface and gives cybercriminals more potential entry points for attack. Or, you can limit the systems you use and minimize your attack surface.

Why Server Hardening Is Important

Hardening your servers allows your company to remove attack vectors. Cybercriminals constantly explore ways to attack servers, and your business must plan accordingly. Failure to do so can result in a server attack and data breach that impact your business, its employees, and its customers.

How Server Hardening Works

Server hardening consists of measures used to protect your business servers' data, ports, and other components. It also accounts for protection across your firmware, hardware, and software layers.

There are many measures that you can use to harden your servers, including:

- Patching and updating your operating systems regularly
- Updating third-party software required to run your servers in accordance with industry security standards
- Requiring users to create and maintain complex passwords that consist of letters, numbers, and special characters and update these passwords frequently
- Locking an account after a set number of failed login attempts
- Deactivating certain USB ports when a server boots
- Leveraging multi-factor authentication (MFA)
- Using AES encryption or self-encrypted drives to hide and secure business-critical information
- Utilizing antivirus and firewall protection and other advanced security solutions

Server Hardening Standards and Guidelines

NIST's Special Publication 800-123 offers standards and guidelines for hardening servers, such as:

- Create a security plan
- Patch and update your OS
- Remove or deactivate unnecessary applications, services, or network protocols
- Configure OS user authentication
- Utilize authentication and encryption technologies

The CIS Benchmarks also provide server configuration guidelines that are commonly used by businesses, educational institutions, and government agencies.

Server Hardening Checklist

Here are the factors to consider when you harden your servers:

- User accounts and logins
- Server components and subsystems
- Software and application updates and vulnerabilities
- Server clocks and timestamps
- Networks and firewalls
- Remote access security
- Log management

Server Hardening Process

1. Manage Access to Your Servers and Critical Infrastructure

Make sure your servers are in a safe location. Only authorized workers should have access to your servers. Provide these workers with ongoing server hardening training and updates so they can protect your servers 24/7/365.

Establish user access controls to limit access to business-critical apps and files. Also, secure routers, switches, and other equipment across your IT infrastructure and restrict physical access to them.

2. Set Up a Firewall

Use a firewall to separate your business network from external sources. In addition, create firewall rules and audit them periodically. Your firewall and firewall rules should always ensure your network is protected against malicious applications and unauthorized access.

3. Manage Your Configurations

Find out what systems are running on your servers and how they're being used. Next, set up a system for managing configurations across your IT environment.

4. Protect User Accounts

Verify that all server usernames and passwords are private and secure. Require users to establish unique passwords and update them regularly. Utilize MFA to ensure users must complete multiple authentication steps to verify their identities.

5. Patch Vulnerabilities

Apply software patches as soon as they become available. Establish a patch management process so you can keep an eye out for patches and update your software frequently.

6. Eliminate Unnecessary Software and Applications

Look for software and applications that are no longer in use and remove them. This eliminates attack vectors and reduces your business' attack surface.

7. Make a Backup Plan

Back up your server data to a local server, cloud server, or hybrid system. Establish multiple backup solutions, too. This gives you several options for recovering your server data following a cyberattack or data breach.

8. Continuously Monitor Your Servers

Monitor server logins and find out who is accessing your systems, when they are doing so, and other relevant information. Collect and assess server data and insights so you can continuously identify ways to bolster your security posture.

Server Hardening Tips

1. Encrypt Your Data

Use encryption technologies across your data. Protect this information using passwords, keys, and certificates.

2. Keep Your Software and Apps to a Minimum

Think about whether you actually need software or applications before you download them. If the answer is yes, download the software or app and keep it up to date.

3. Set Up Servers for Different Network Services

Run each network service on its own server. That way, if a server is breached, only one network service is affected.

4. Track Your Configurations

Create an inventory for your server configurations. Your inventory should include documentation about each configuration, along with any changes to it. Also, perform configuration testing and track the results of it. Review and update your server configuration inventory regularly as well.

5. Conduct Risk Assessments

Establish a risk management plan and conduct testing to understand the current state of your server security. Perform risk assessments to identify security gaps and figure out the best ways to address them. These assessments can be performed by your internal IT security team, or you can partner with a third-party security vendor.

6. Enforce Strong Passwords

Make sure your workers follow your company's password management policy. Do not allow employees to use common password terms that cybercriminals can easily guess. Workers should set up complex passwords and never share them with anyone. They should also avoid keeping passwords on desks or in any public areas.

7. Teach Your Workers About Server Hardening

Educate your employees about server hardening, how it works, and why it is important. Regularly review your server hardening training and update it as needed.

8. Continue to Look for Ways to Improve

Meet with members of your IT security team, C-suite executives, and other business professionals to discuss cybersecurity. Together, staff across your business can look for ways to protect against all types of cyberattacks and upgrade your security posture.

Protect Your Server Workloads with Sophos

Sophos Intercept X for Server delivers server and container protection on premises, in data centers, and in the cloud. It works across Linux, Windows, and hybrid and multi-cloud environments and is integrated into Sophos Central, which offers a unified console for managing all of your Sophos security products.

Key features of Sophos Intercept X for Server include:

- Anti-ransomware protection
- Cloud security posture management (CSPM)

- Extended detection and response (XDR)
- Managed detection and response (MDR)
- Server lockdown

Sophos Intercept X for Server can be customized to secure your business across your server environments.

Learn More

Related security topic: What is XDR in cybersecurity?