What to Do After a Server Attack

A Step-by-Step Guide

Table of Contents

1. Stay Calm and Don’t Panic

Why? Panicking can lead to hasty decisions that might make the situation worse. When you first realize your server has been attacked, it’s natural to feel a surge of anxiety or fear. However, it’s crucial to remain calm and approach the situation methodically.

[Graphic source: PNGITEM]

- ✓ **Take a deep breath.** Allow yourself a moment to collect your thoughts. Clear thinking is your best tool right now. Panicking can cloud your judgment and lead to rash decisions that may further compromise your server’s security.

- ✓ **Understand the situation.** Before taking any action, try to gauge what’s happening. Is the server still operational? Are users reporting issues? The more information you have, the better prepared you'll be to communicate effectively with your IT or cybersecurity team.

- ✓ **Resist the urge to tamper with the server**. Uninformed actions could erase crucial evidence or even worsen the situation. Avoid making changes, running any scripts, or attempting to "fix" things on your own. Your priority is to preserve the current state of the server for investigation.

- ✓ **Remember, you’re not alone.** Many businesses and individuals face server attacks, and there are established procedures for handling them. Your IT team or a cybersecurity professional can guide you through the next steps. Trust in their expertise and remain patient as they take over the situation.

- ✓ **Focus on what you can control.** While the attack itself might be beyond your control, how you respond is entirely up to you. A calm and measured response can significantly mitigate the impact of the attack.

2. Disconnect the Server from the Network

Why? This stops the attack from spreading or causing more damage. Once you've taken a moment to calm down, your next priority should be to isolate the compromised server from your network. By disconnecting the server, you limit the attacker's ability to spread the attack, access more data, or further harm your systems.

[Graphic source: router-switch]

[Graphic source: drfone]

- ✓ **Unplug the network cable or disable Wi-Fi.** If the server is connected via Ethernet, unplug the cable to immediately cut its network access. For wireless connections, disable the Wi-Fi adapter to stop the server from communicating over the network.

- ✓ **If you're unsure how to disconnect, turn off the server.** As a precautionary measure, powering down the server is a safer alternative if you're not familiar with disconnecting it. This will halt any ongoing activities and prevent further issues, though it may impact other services.

- ✓ **Inform your team.** Let your colleagues know about the server disconnection to manage expectations and coordinate any necessary responses.

- ✓ **Document the disconnection.** Note the exact time when the server was disconnected to aid in the investigation and analysis of the attack.

- ✓ **Await further instructions.** Do not reconnect the server until you receive guidance from your IT or cybersecurity team to ensure that it is safe to do so.

3. Inform Your IT or Cybersecurity Team Immediately

Why? Your IT or cybersecurity team has the expertise and tools to handle the situation effectively. As soon as you realize your server has been compromised, reaching out to them is crucial.

[**Graphic source: ALLCore**]

- ✓ **Contact your IT or cybersecurity team right away.** Use email, phone, or instant messaging to notify your team immediately. Time is critical in containing the attack and minimizing damage.

- ✓ **Provide relevant details.** Share what you know about the incident, including when you noticed the issue, any unusual activities, and actions you've already taken (like disconnecting the server). Detailed information helps them assess the situation quickly.

- ✓ **Follow their instructions closely**. Your team may ask you to perform specific actions or avoid certain activities. It's important to follow their guidance precisely to prevent further harm.

- ✓ **Stay available for communication.** Keep your phone or email handy for any follow-up questions or instructions, as they may need additional details to resolve the issue.

4. Document Everything You Observe

Why? Detailed documentation is essential for the investigation. Recording your observations can provide valuable insights for your IT or cybersecurity team.

[Graphic source: CSM]

- ✓ **Note unusual activities.** Write down anything out of the ordinary, such as strange behavior, error messages, or unexpected system changes. Every detail might be important.

- ✓ **Record the timeline.** Document when you first noticed the issue and any actions you've taken since. A clear timeline helps in understanding the sequence of events.

- ✓ **Take screenshots if safe.** Capture screenshots of unusual activity, error messages, or alerts if it's safe to do so. Visual evidence is often very helpful.

- ✓ **Log your actions.** Keep track of steps you've taken, like disconnecting the server or notifying your team, along with the times these occurred.

5. Avoid Using the Server Until Help Arrives

Why? Using the server could worsen the problem or interfere with the investigation. After taking initial steps, it's crucial to leave the server untouched until your IT or cybersecurity team can assess the situation.

[Graphic source: makeuseof]

- ✓ **Don't log in.** Avoid logging into the server, as it could trigger processes that might escalate the attack or destroy evidence.

- ✓ **Don't restart or shut down the server.** Restarting or shutting down can disrupt important logs needed for investigation. Wait for professional guidance before making any changes.

- ✓ **Avoid any tasks on the server.** Refrain from running scripts, checking logs, or making modifications, as these actions could complicate the investigation.

- ✓ **Communicate the status.** Inform your team that the server is off-limits until further notice to prevent accidental interference.

- ✓ **Wait for instructions.** Be patient and await further guidance from your IT or cybersecurity team.

6. Review Your Backup Strategy

Why? Regular backups are crucial for recovering data after an attack. Now is the time to assess your backup practices.

[Graphic source: makeuseof]

- ✓ **Verify your latest backup.** Ensure your most recent backup is complete and securely stored.

- ✓ **Keep backups current.** Regular updates reduce the risk of data loss in future attacks.

- ✓ **Secure your backups.** Use offsite or cloud storage to protect backups from being compromised.

- ✓ **Plan restoration carefully.** Coordinate with your IT team on how and when to restore data safely.

- ✓ **Improve your strategy if needed.** Evaluate your backup approach based on this incident and make necessary adjustments.

7. Cooperate with the Investigation

Why? Your cooperation is essential for a thorough and effective investigation. The more information you provide, the better your IT or cybersecurity team can respond to the incident.

[Graphic source: strategywisehr]

- ✓ **Answer questions honestly.** Provide clear and truthful responses to inquiries from your IT or cybersecurity team. Your input helps them understand the scope and impact of the attack.

- ✓ **Share all relevant information.** Offer any logs, notes, or screenshots you've taken. Every piece of data can be valuable in piecing together what happened.

- ✓ **Follow up promptly.** Respond quickly to any requests for additional information or clarification to avoid delays in the investigation.

- ✓ **Maintain confidentiality.** Avoid discussing details of the incident outside the investigation team to protect sensitive information.

- ✓ **Stay engaged.** Be available for ongoing communication as the investigation progresses.

8. Learn from the Incident

Why? Understanding what happened helps you strengthen your defenses and prevent future attacks. Every incident is an opportunity to improve.

[Graphic source: College of Engineering Safety]

- ✓ **Review the incident report.** Attend a debriefing session or read the report to understand what occurred and why. Knowing the root cause is essential for making informed decisions.

- ✓ **Implement recommended changes.** Follow through on security improvements suggested by your IT or cybersecurity team. This may involve updating software, changing passwords, or revising policies.

- ✓ **Update training and awareness.** Use the incident as a case study for training, helping your team recognize and respond to threats more effectively.

- ✓ **Evaluate and improve your security posture.** Consider whether your current security measures are adequate and make adjustments as needed to prevent similar attacks in the future.