wickr.com

7 Steps to Take During a Cyber Attack | AWS Wickr

Wickr Staff

5–7 minutes

If your organization becomes the victim of a cyber attack, what steps should you take? With cyber attacks on the rise and cybercrime expected to cost $6 trillion globally in 2021, it's important that you have a plan for how to respond if your company is attacked.

Detecting a Cyber Attack

Before you can stop a cyber attack, you have to recognize that it's happening. This isn't always easy — cyber attackers are good at not being found. As detailed in IBM's Cost of a Data Breach Report 2020, companies on average take 207 days

to identify a data breach and another 73 days to contain the attack. A lot of damage can be done before a cyber attack is recognized and contained.

For example, the recent SolarWinds cyber attack on hundreds of private companies and government agencies went undiscovered for more than nine months. At this writing, the full extent of the attack has yet to be tallied, and the breach is ongoing.

Ransomware and other active attacks, such as DDoS attacks, are easiest to detect, as their effects are the most immediate. Passive attacks and cyber espionage are more difficult to spot, as the attackers go to great lengths to hide all traces of their presence. The most effective of these cyber attacks are so sanitized that they're not discovered for months after the initial penetration.

How, then, can you detect a cyber attack in progress? The SolarWinds attack was discovered when one of the victims, FireEye, identified the theft of its cybersecurity tools. Other attacks have been discovered by observing higher-than-normal network usage, unusual password activity, or

missing data.

7 Essential Steps to Manage a Cyber Attack

When you discover that your company is under attack, there are seven essential steps you should take. The goals are to both stop the attack and mitigate its effects.

1. Mobilize Your Cybersecurity Response Team

The first thing your company should do when a cyber attack is discovered is to mobilize your cybersecurity response team. This should be a team of cross-discipline professionals trained in protecting your business from such attacks. It's important that each team member has been properly trained in his or her role and knows precisely what to do in the event of an attack.

2. Identify the Type of Attack

For the cybersecurity response team to react

appropriately, they must properly identify the type of attack. Once you know what type of attack is occurring, you can know where to focus your attention and how best to contain and recover from the attack. You need to know not just the type of attack but also the likely source, the extent of the attack, and its probable impact.

3. Contain the Breach

Most passive attacks are designed to provide the attackers with a persistent backdoor into your systems, so that data can continue to be extracted over time. It's important to identify and shut down all access the attackers may have to your system. The same is true, obviously, if your company is the victim of a more active attack.

Whatever type of cyber attack you experience, your team should promptly move to:

- Disconnect the affected network from the Internet
- Disable all remote access to the network
- Re-route network traffic

- Change all vulnerable passwords

  The key is to completely deny the attackers access to your system. You can then work to return the system to a hopefully more secure working condition.

4. Assess and Repair the Damage

Once the attack has been contained, you need to determine which (if any) critical business functions have been compromised, what data has been affected by the breach, which systems have been illicitly accessed, and whether any unauthorized entry points remain. Systems may need to be reinstalled, compromised data may need to be restored from backup copies, and any damaged hardware repaired or replaced.

5. Report the Attack

It’s also important to promptly report the attack to the proper authorities. Immediately contact the FBI and state and local law enforcement offices. You’ll also want to report the attack to the Secret

Service's Electronic Crimes Task Force, as well as the Internet Crime Complaint Center and the Federal Trade Commission. If your company has cyber liability insurance, contact your insurance carrier for advice and support.

6. Communicate with Customers

Work with your PR department to determine how best to manage the public impact of the event. Your customers will need to be notified, especially if the attack impacted any customer data. It's also important to issue a press release regarding the incident. You need to be upfront and transparent about the attack in order to maintain public trust.

7. Learn from the Experience

Finally, your organization needs to learn from the experience. Do a thorough investigation and determine how to change your systems and procedures to ward off future attacks. Use this incident to get smarter and stronger about your company's cybersecurity.

Reduce Your Risk of Cyber Attack with Wickr

A secure collaboration platform can significantly reduce your company's risk of a cyber attack. Wickr offers full control, total compliance, and complete security with end-to-end encryption for all communications and file sharing.

***Contact us today* to learn how Wickr can help protect your organization from cyber attacks.**