Understanding More About Cyberattack - 4 Steps of Prevention

TechRounder PDF Edition

Live article: https://www.techrounder.com/security/understanding-more-about-cyberattack-4-steps-of-prevention/

By Vipin PG | Published January 13, 2023 | Updated March 8, 2026 | Format: Explainer | 5 min read

In brief

No business is 100% safe from a cyberattack. Whether it’s a small brick-and-mortar business or a large corporation, there’s always a risk of someone trying to break in and steal sensitive information.

No business is 100% safe from a cyberattack. Whether it’s a small brick-and-mortar business or a large corporation, there’s always a risk of someone trying to break in and steal sensitive information.

However, it is not impossible to reduce the risk of being hacked and prevent severe damage resulting from cyber threats. And the best way to do so is to understand the anatomy of a cyberattack. By knowing how they arise, you can better prepare and defend against them when the time comes.

In this post, we will help you understand the anatomy of a cyberattack and lead you through the 4 exceptional steps of prevention. From explaining how to identify vulnerabilities to patching them up, we’ll cover everything you need to know to keep your business safe. Let’s begin!

What is a Cyberattack?

A cyberattack is a security breach that occurs when an attacker gains access to the user’s system or network and tries to alter or destroy their workflow. Hackers deploy cyberattacks for various reasons, including financial gain, political or ideological agendas, or the desire to cause havoc and steal the user’s sensitive data.

Although there are many different types of cyberattacks, they all typically follow a similar pattern. That said, they have the same anatomy, and it often looks like this:

Reconnaissance: In this phase, the attacker gathers information about their targets, especially focusing on network architecture and vulnerable systems.

Weaponization: The next step allows the attacker to create malicious software (e.g., malware) specifically tailored to exploit weaknesses in the target system.

Delivery: Now, the hacker delivers the malware to the target system, mainly using social engineering techniques to trick users into executing it.

Exploitation: The malware is executed on the target system, allowing the hacker to gain access and begin with the malicious plan development.

Installation: Now that the attacker has access to the system, they can install additional malware or tools to extend their control.

Command and Control: Finally, the hacker remotely controls the compromised system to perform their desired actions. This may include exfiltrating data, launching attacks against other systems, or using the system as a pivot point to attack other systems on the same network.

However, when it comes to cyberattacks, there is no one-size-fits-all. Although they share similar characteristics and anatomy, each attack is unique and can vary significantly in scale, scope, and complexity. Therefore, it's essential to learn how to identify each of them and ensure that your business IT ecosystem is fully protected from scams and cyber threats that arise every day.

Now that we understand the basic anatomy of a cyberattack, we can move on to the 4 essential steps for preventing them and keeping your business safe in the long run.

How to Prevent Cyber Attacks?

As we mentioned, the first step in prevention is understanding the anatomy of a cyberattack.

But there are other steps you can take to prevent your business from being attacked. We'll highlight the four most efficient methods:

1. Upgrade Your Passwords

Weak passwords can help hackers gain your sensitive information more easily. And while users prefer using simple, easy-to-guess passwords to secure their essential accounts, that is never a good option.

Here is why.

Passwords open the door to many vulnerabilities, allowing attackers to enter sensitive systems seamlessly. Reckless password sharing or reusing phrases is often the most common reason for data breaches, and it's important to avoid it. But there is a simple solution even for the lazy ones - a password manager.

A password manager allows you to generate strong and unique passwords for your sensitive accounts while letting you share them with others without risks. In addition, features for field autocomplete mitigate brute force and similar attacks that could enter your system through passwords.

Once your passwords are updated, you can prevent cyber threats and take your account protection to new heights.

2. Educate your Employees About Cybersecurity Threats

Although you've implemented the best password protection measures, firewalls, intrusion prevention/detection tools, encryption, and similar, educating your employees about cybersecurity is a must.

Make sure to educate your employees daily by helping them understand the risks of cyber threats and providing them with instructional materials and courses that might allow them to acquire the necessary knowledge and skills.

Besides teaching them how to detect and respond to security threats, it's essential to have adequate policies in place in case of a cybersecurity event. Your company can mitigate long-term consequences, lawsuits, and financial loss risks.

3. Update Your Software Regularly

Businesses that develop in the digital era use a broad range of software solutions for accounting, banking, customer relations, and money transfer. However, even such tools can be a potential threat if they don't run on the latest software version.

When the device runs on outdated software, hackers can easily detect the flaws and use them to access the system's core. To prevent that, installing the latest updates as soon as they're released is essential. Since each comes with the newest security patches, you can be sure that you're not at risk of zero-day or similar attacks.

And if the developers no longer provide upgrades for particular software, make sure to deinstall it and start using another product.

4. Back-Up Your Data Regularly

Sometimes, cybersecurity events are impossible to avoid. But losing all your data is preventable.

Don't forget to perform regular data backups to ensure it's safe even if hackers attack your system. You can store copies of your valuable data either in the cloud or in on-premise solutions. That way, you can recover them at any time.

Conclusion

By understanding how cyberattacks work and their anatomy, you can devise the most efficient strategies to avoid them and protect your business from data breaches that could cost it money and reputation.

And remember - hackers often target small businesses due to their weaker cyber protection. You don't need to be one of them - understand the importance of SMEs' cybersecurity and start upgrading yours today!

References

1. safetydetectives.com - best-password-managers - https://www.safetydetectives.com/best-password-managers/

2. spiceworks.com - it-security / cyber-risk-management - https://www.spiceworks.com/it-security/cyber-risk-management/articles/training-employees-against-cyberattacks/