Three of the Most Damaging Kinds

of Cyberattack and How to Counter Them

Three of the Most Damaging Kinds

of Cyberattack and How to Counter Them

Cybersecurity is a top concern for nearly every size and type of organization, from rural small businesses to federal and international government agencies. Cybercriminals grow more dangerous every year because their tools continue to evolve in complexity and sophistication. The result is more cyberattacks of diverse varieties that are even more expensive for their victims.

Fortunately, the success of most cyberattacks still rely largely on the victim's complacency and ignorance, which means we can protect ourselves by learning more about cyberattacks, performing simple defensive measures, and remaining vigilant. Let's take a look at three of the most dangerous types of cyberattacks and the relatively simple things we can do to protect ourselves.

1. Ransomware

This type of malware is a newcomer on the scene compared to “older” cyberattacks like viruses and Trojans. Instead of destroying your data and making your network inoperable, ransomware locks down and encrypts data that is vital to your operations, such as financial records and software platforms.

After your data is locked away, the malware program demands you pay a ransom to the cybercriminal, usually in difficult-to-trace cryptocurrencies like bitcoin. But even if a victim pays the ransom (which can be a few thousand to millions of dollars), the cybercriminal usually just destroys the data anyway, or simply disappears without unlocking the files.

How to Counter It

Ransomware is delivered via many of the same ways other malware is. Most commonly, it hides in seemingly innocuous emails as attachments or even fileless malware, which requires no executable and leaves no footprint. Other ransomware is delivered through unsafe sites where any click could lead to infection.

Fortunately, by blocking these transmission vectors with filtering software, you can keep ransomware out of your systems. Have an IT professional set up email filtering programs that scan incoming messages for signs of ransomware and block them from being opened. Internet browsers and other web filtering software can also be deployed to prevent computers on your network from accessing these sites.

2. Spear Phishing

You may have heard of phishing before; it's a scam that's almost as old as email itself. But these days it's a bit more sophisticated and, unfortunately, successful. Spear phishing cybercriminals first collect personal information about their targets, then they craft targeted emails that appear legitimate by using names the victim recognizes or claiming to be an employee of a trusted organization. These emails are much more believable than the generic phishing emails of the past.

Once the victim believes the spear phishing email is legitimate, they might be led to click on infectious malware or tricked into providing login credentials the cybercriminal can then use to access private data. By earning the trust of the victim, scammers get far better access to their victims, meaning far greater losses.

How to Counter It

Email filtering software configured by an expert is also effective here, but it isn't enough due to the sophistication of the attack. Everyone who uses your network must remain vigilant and know how to spot a spear phishing email. Some telltale signs include:

- Sender's email address is similar to a legitimate one, but with small variations
- Message is brief, but claims that an urgent matter needs the recipient's attention
- Message contains unfamiliar links or strange lines of code
- Message uses full names of recipients or senders instead of casual or nicknames
- And many more

Ideally, everyone on your network should receive instruction from a cybersecurity professional to learn all the warning signs and how to deal with phishing emails.

3. Zero-Day Attack

These attacks are different from phishing scams or malware because they rely on weaknesses in the software you use every day. Newly released software and firmware (hence, “zero day”) such as a Windows operating system or even anti-malware apps sometimes have vulnerabilities cybercriminals can exploit to gain unauthorized access to networks or infect them with malware.

These weaknesses are usually found and fixed through software updates and upgrades, but there is still a window of opportunity when these attacks are effective. Furthermore, every day a software program goes un-updated or unpatched keeps that window open for longer. As these attacks are all but untraceable since they are “allowed” in, the damage they can do is monumental.

How to Counter It

The best way to counter zero-day attacks is to always be one step ahead. Stay abreast of new vulnerabilities that are discovered, and ensure that ALL of your software and firmware are up-to-date and completely patched. Simply turning on auto-update settings will not keep you safe, as many programs do not have them, people sometimes ignore or turn them off, and sometimes the program checks for updates too infrequently.

Staying Protected

There are many ways to defend yourself and your network from cyberattacks, but professional help is always best. After all, a cybercriminal's full-time job is to get your money, so getting a full-time cybersecurity expert to prevent this is the best option.

An in-house IT technician will be able to set up, maintain, and operate your software defenses as well as teach the users on your network to do their part to prevent cyberattacks. If you can't afford to hire full-time cybersecurity staff or just want more protection, consider partnering with a Managed IT Services Provider (MSP).