The Biggest Cybersecurity Risks Business Owners Are Hedging Against

Devolutions

EVERYONE IS AT RISK WHEN IT COMES TO CYBER THREATS

You may think that only the big corporations need to take care of cybersecurity. Unfortunately, everyone is at risk when it comes to cyber threats. Here are some of the bigger threats you should protect your business against.

Ransomware

Ransomware is the digital form of racketeering. All it takes is one digital security mistake and your company may grind to a halt for weeks as you work to resolve the crisis.

Ransomware encrypts all files on your servers and computers, barring you from doing business or recovering the files. To restore your files, you have to pay off the digital racketeers.

The most notorious version of ransomware, NotPetya, was an organized attack on companies that are critical to Ukraine's economy and infrastructure, including bus stations, banks, and power grids. Less ambitious hackers may target companies or private PCs that lack sufficient security measures.

One of the things that can allow hackers to get into your system is not having an up-to-date antivirus or falling for a phishing attempt.

Endpoint Attacks

The culture of bringing your own device to work has its benefits, but it also has pitfalls. Whereas it's hard for hackers to get into a closed system from the outside, it's comparatively easy for hackers to infiltrate an employee's personal laptop. But once they connect to your main servers in the office, the virus can spread quickly. This is why it's imperative to educate your employees on safety protocols if they're bringing their own devices to work.

Third-Party Attacks

Your website may be protected by the latest practices, but that might not be enough to stop hackers. Third-party software can be a weak point that allows malware to spread. If you're using a compromised plugin or your web host is not secure enough, it can be the gateway for malware.

XSS Attacks

Cross-site scripting can cause your clients to lose vital private information like banking details, while also allowing hackers to access your website's admin panel. On both fronts, this is bad for business — either directly via financial hit or indirectly through reputation loss. Sanitizing the input on your website and making sure the output is encrypted will prevent most XSS attacks.

Database Hacks

Earlier this year, the planet's biggest social network, Facebook, was careless enough to let several huge databases sit without password protection, causing the personal information of over 400 million users to be leaked. While your organization may not be so careless, bad database protection can result in outsiders getting access to highly-sensitive data.

The reputation loss and the damage this will do to your business may be hard to reverse. As Jessica Neilsen, CEO of the professional writing agency Essay Writer, says: "Our servers host information that, if released, can be devastating for our clients' careers. This is why we make sure to always have a backup and encrypt users' sensitive data to prevent hackers from getting to it."

Creating a strong password that is not a date or somebody's name is also a good move. It would take a thousand years to crack a password that consists of 8 numbers and letters in both cases, and it's not a difficult task to create one.

Cryptojacking

This type of cybersecurity threat is not as easy to recognize. Hackers don't try to get access to your database; they simply want your computing power in order to mine cryptocurrency.

Although this may seem harmless, mining crypto takes a huge deal of power and electricity, which can, over time, cause your servers to overload. This will significantly slow down your website, causing revenue to drop as hackers make a fortune off of you.

Protecting against this security threat includes making sure your website is not a good target for SQL injection and educating your employees about the potential danger involved in cryptojacking.

Phishing

Phishing is one of the oldest and most effective hacking techniques. It exploits human error, which is far less reliable than any code. Most of the threats on this list use phishing to get access to your system, so knowing how to prevent phishing strategies is key to your business's security. The first thing you should teach your employees is to always know who's email you're opening, which means never running suspicious files.

Insider Threats

You may be surprised to learn that most security threats come from people you trust, not hackers. Former employees who have a grudge, a current employee who has malicious intentions, or a remote employee whose laptop gets hacked, can be just as dangerous as poor website protection.

This means that a manager you hired or a software engineer you let go may voluntarily or involuntarily (i.e. by negligence or ignorance) lead your business into a security crisis. You have to work on onboarding and offboarding procedures to make sure your personnel doesn't turn into a security threat.

Conclusion

Cybersecurity risks are very real, regardless of whether you own a small business or a corporation. Protect yourself from the threats you find in this article, and you'll cover the majority of risks on the web.