WHY HACKERS TARGET SMALL BUSINESSES

SysGen
solutions group

WHY HACKERS TARGET SMALL BUSINESSES

Nearly half of cybercriminals target their attacks at small businesses. In fact, 77% of data breaches occur at companies with less than 1000 employees. Why is that?

While smaller sized companies may have not been the prime target for financial or data threats in the past, that fact is no more. Today, small companies are the perfect suspects for a security attack.

Hackers know the market. Taking advantage of the fact that smaller companies used to fly past the radar, cybercriminals are now taking small to medium-sized businesses by surprise.

In 2015, nearly half of global attacks were against companies with less than 250 employees, as cybercriminals set out to exploit digital weaknesses. Over the past four years, small firms have become a more attractive target, especially as larger companies have improved security systems, locking out hackers.

Security breaches statistics are just as unpleasant as the repercussions. Costs for per an incident at small businesses average $60,000 and $1,400,000 at larger companies.

These hefty fees include the cost of lost operations, IT support to resolve the incident, IT services to implement preventative measures, and the loss of business opportunity. What's worse is that 60% of businesses that suffer a breach find their ability to function severely impaired. The costs and chance of data breach are high.

WHAT ARE THE MOST COMMON TYPES OF ATTACKS?

The most prevalent attacks against small businesses are phishing and password attacks.

Phishing attacks are when hackers send emails pretending to be reputable companies to con employees into sharing passwords, and credit card information. Spam and malware attacks are the most common types of phishing attacks on small firms.

Malware is initiated into computers when a user downloads a program laden with malicious software.

Spam, on the other hand, is introduced through emails and have unexpected attachments, file sharing links, unsolicited advertisements, or

compelling messages creating a sense of urgency.

The second most common cyber attack on small businesses is password attacks. There are three main types of passwords attacks: brute-force, dictionary and key logging.

A brute-force attack is when a hacker guesses at passwords until access is gained. Dictionary attacks are when a program tries different combinations of dictionary words. Key logging tracks all user keystrokes, including login IDs and passwords.

Whether it's malware, spam or a password attack, the hacker's intent is to gather sensitive information and gain access to private computer systems.

So, how can small businesses stop this from happening?

HOW SMALL BUSINESSES CAN PREVENT HACKER ATTACKS

Protecting your business is easier than you think. Here are 5 IT security solutions to prevent attacks and mitigate negative impacts:

1. Anti-virus is the first step to blocking out hackers. Anti-virus software continually collects, analyzes and correlates data, ensuring protection against most types of malware.

2. Firewalls should also be implemented with hardware and software. This adds another layer of protection by preventing an unauthorized user from accessing a computer or backup.

3. Encryption software is a focused solution, specifically to protect highly confidential files such as employee records, customer information and financial statements.

4. Two-step authentication and password security software help reduce the likelihood of password cracking in workplaces.

5. A data backup solution is crucial security solution. If any information is lost or compromised during a breach, it can easily be recovered from an alternate location with backup software.

With all of these IT solutions to protect your business, one of the most important things to remember is to ensure they're kept up-to-date to fight off the latest and most advanced attacks.

While targeted IT security solutions are the foundation of enhanced security for your

organization, user education and policy development complete the picture.

80% of data breaches are caused by human error. Top security threats come from accidental actions by staff, including mistakenly sharing data, opening anonymous links and attachments.

The top 2 actions to take to support users are education and policies:

1. User training on how to identify security threats, and the top causes of malware and viruses is fundamental in prevention. Keeping employees aware of the latest threats is highly effective education and security enhancement.

2. Policies help reinforce user practices. Company-wide policies help reduce the likelihood of attack. Requiring strong passwords and frequent changes are two great examples of how policies complement employee education.

GET PREPARED FOR ATTACK

With the high rates of attacks on small businesses, it's not if, but when a hacker will strike. SysGen takes a comprehensive approach to security services by focusing on technology, people, and policies.

To help set up an all-encompassing security solution, contact SysGen for an IT security consultation and to learn more about security best practices at small to mid-sized businesses.