SMBs Beware: 3 Reasons Why Size Doesn't Matter for Cyber Criminals

Devolutions

FOR MANY THINGS IN LIFE, BIGGER IS BETTER. BUT WHEN IT COMES TO TARGETING VICTIMS, THE MANTRA FOR CYBER CRIMINALS IS "SIZE DOESN'T MATTER."

For many things in life, bigger is better. But when it comes to targeting victims, the mantra for cyber criminals is "size doesn't matter." Everyone is fair game, from large enterprises to small firms.

The problem, however, is that while big companies are adding tools to improve their network defense system, some SMBs aren't making security a top priority — even though they're increasingly being targeted by cyber criminals.

Here are 3 reasons why SMBs need to take security very seriously ASAP:

1. TODAY'S HACKERS ARE FINANCIALLY MOTIVATED

In the past, most hackers wanted to destroy machines and wreak havoc. While this obviously caused financial damage, that wasn't the main purpose of the attack. However, today's hackers are very different than their predecessors. **They're financially motivated, and they focus with laser-like precision on stealing data** that they either use to commit identity theft, or sell in the cyber underground.

2. THE COSTS CAN BE MASSIVE

There are many costs of a data breach, including: incident investigation, remediation, replacement, customer notification, crisis management, regulatory fines, penalties, and possibly lawsuits as well. According to Kapersky Lab, **the average cost of a data breach in an SMB is now $117,000 per incident**. And that's the average — for many SMBs, the cost is significantly higher.

3. THE REPUTATION DAMAGE CAN BE DEVASTATING

The reputation damage caused by a data breach can be devastating. Ironically, this is one of those situations where bigger is better. For example, while Target and Sony each **took a massive reputation hit due to their respective data breaches, neither of them came close to disappearing** from the business landscape. However, most SMBs can't say the same thing. If their brand gets associated with a breach, then it may be impossible to regain trust in the marketplace. Research by the U.S. National Cyber Security Alliance found that **within 6 months of a cyber attack, 60% of small firms are forced to go out of business.**

The Moral to this Scary Story

We aren't here to scare anyone. However, data breaches ARE frightening and costly. And so, here's what we urge you to realize right now:

Don't assume that you're safe because you're a small or mid-sized business. Remember: size doesn't matter. **You have valuable data in your software and systems (including customer data), and cyber criminals want to get it.**

On a more positive note, there are many ways to improve your cyber security. Develop a robust password policy, avoid common password mistakes (like storing passwords in your browser), deploy these essential security tools in your environment, and use a proven password manager like Devolutions Server.

What's Your Advice?

If you work in an SMB, please share your advice on what your company is doing to stay safe.