Cybercriminals Target SMBs, But New Technology Helps Fight Them Off

Contrary to popular belief, big companies are not the only favored targets of cybercriminals. SMBs are just as attractive.

The small and midsize business (SMB) market is a target-rich environment for cybercriminals, and the pandemic-spurred surge in remote work has elevated the threat level significantly. Hackers are taking advantage of confusion triggered by the coronavirus, and data breaches almost tripled in the first quarter of 2020.

Despite the danger, only about 15 percent of SMBs have any kind of cybersecurity defense at all. Most small businesses don't have an IT specialist on staff. "Even if they do, there is a slim chance that person is a qualified cybersecurity expert," says Jack Blount, president and CEO of INTRUSION, a cybersecurity company.

Compounding the problem is the misconception that cybercriminals are only interested in targeting big businesses. "This couldn't be more untrue," Blount says. Today, most cybercrime is driven by artificial intelligence (AI) algorithms and supercomputers that simply attack every IP address on the internet, around the clock. "The massive and virtually defenseless SMB market is vulnerable and tempting."

Most dangerous threats

Virtually any type of cybercrime or malware can put a company out of business, but the most dangerous are theft of proprietary data, ransomware, identity fraud, and phishing. The average cost of a ransomware attack in the SMB market is estimated at $133,000, and attacks occur every 14 seconds. However, theft of proprietary data is a more dangerous threat because it's more likely to result in bankruptcy for the business, Blount notes.

The best way for SMBs to protect themselves from these threats is with "defense in depth," which uses layers of technology to create a more secure environment. For large organizations, that might entail 10 or more layers of cybersecurity architecture, which is out of reach for most SMBs. For them, Blount recommends a three-layer architecture, which is neither complex nor expensive.

The first layer is a firewall, which every business should have already. The second layer is a network appliance that can open and inspect all packets of data attempting to enter or exit the business's network. The third layer is a client-based solution that can protect computers when they are not connected to the business's network, such as Symantec, McAfee, and others. All layers of protection should be updated constantly to keep pace with the ever-changing landscape of cyber crime.

Always-on protection

Ideally, once the network appliance in the second layer of architecture inspects the data packets, it should be able to identify and kill potentially dangerous connections without user involvement. "INTRUSION Shield is updated daily to ensure it is always using state-of-the-art technology and the latest information to protect its users' networks. It is the only real-time, AI-based cybersecurity solution. It's low-cost, hands-free, and uses AI to get smarter, faster, and more efficient every minute," Blount says. And when SMBs are fighting cybercriminals, every minute counts.


CYBER SECURITY HAS FAILED,
IT'S TIME FOR A REAL DEFENSE.
INTRUSION.COM/SHIELD
INTRUSION