INSIGHTS

One Brightly Cyber

SMES – A GROWING CYBER TARGET

BY JAY BORDEN

SMEs, Small and Medium Enterprises, often think they are too small to be targets for cybercriminals. But that is far from the case. Cybercriminals always saw SMEs as targets because most of them have very small or non-existent cybersecurity teams. Many do not have the money for larger teams. Or better defenses or user education. But many don't understand how vulnerable they are.

Regardless of size most businesses keep important information on their customers including name, address, email, purchase history, credit card number, and more. All very desirable information for attackers. Why? Because it can be easily monetized. It can be used or sold to other attackers who want to inflict their own damage, steal identities, steal medical identities, infect the systems with ransomware, etc., etc., etc. You get the picture.

In case you think this is an exaggeration, researchers in multiple cybersecurity firms found that 70% of the security incidents affecting small businesses involved ransomware, while 90% of the cases affecting midsize businesses — defined as 500 to 5,000 employees — involved ransomware.

To be more effective attackers have adopted a new technique to avoid detection. The ransomware is run outside the network. For instance, on a file sharing device that has access to the files on the target company's network. The encryption runs on the target company devices but the encryption is not the ransomware itself, so it avoids detection by anti-malware, and other protective software.

SMEs are becoming even more attractive to attackers leading to an increase in attacks. The reason is simple, many SMEs connect to other, larger companies as part of their supply chain. Those larger companies probably do have well-staffed cybersecurity teams. But an SME in their supply chain typically has access to their systems.

SMES – A GROWING CYBER TARGET

CONTINUED

That access is often an automated variety called a non-human identity. This means there is a username and password or other form of authentication that the systems use to connect to each other. The thing to note here is that there is a valid, working authentication mechanism. This means attackers don't have to break into the larger company, they have a key that lets them in.

The complexity of supply chains means very few companies stand on their own. Everyone orders raw materials or products from other companies and provides their products or services to other companies, their customers. Or they outsource business functions to larger companies.

This is further complicated by those other companies each having their own third parties in their own supply chain. Breaking into one company can provide access to several other companies that may be of more interest to attackers.

Anyone looking to gain entry to a company will use the path of least resistance. In this case the SMEs are viewed as the weak link in the supply chain and that makes them the initial target. This is substantiated by research showing that the percentage of breaches involving third parties doubled from 15% to 30% in one year.

How are the SMEs compromised?
Vulnerabilities as the means of breaking into a system grew 34% and now account for 20% of breaches.

Research shows it took 32 days for an SME to remediate a perimeter device vulnerability and only 54% of the vulnerabilities were fully remediated. This means attackers are more aware of your vulnerabilities than you are!

But, people are still the cause of most breaches. How many of your employees can spot a phishing message? How many use personal devices to connect to company systems? How many use AI? What information is put into the AI systems? Information put into an AI system stays there and can be used to respond to other users. Is it any wonder SMEs are targets?

Visit our website onebrightlycyber.com or call (888) 873-1920 to learn all the ways we help keep you safer.