The Logical Advantage

TeamLogicIT®
Your Technology Advisor

MARCH 2023 ISSUE

Technology Trends

Ransomware Gangs Evolving Tactics

Researchers say most ransomware gangs now use their own or stolen computer code, moving away from a leasing model that made their activities easier for law enforcement agencies to monitor.

For several years, prominent hacking groups profited by leasing malicious software and infrastructure to other bad actors, in what analysts dubbed “ransomware-as-a-service” or RaaS.

Cybersecurity experts say this business model turbo-charged the ransomware trend, spiking the number of successful attacks year-over-year, thereby pushing ransom requirements to new heights. From 2014 through 2021, ransomware payments skyrocketed from $3 million to $1.2 billion.

And that’s just what the Bank Secrecy Act required U.S. institutions to report to the Financial Crimes Enforcement Network. The final tally for 2022 has yet to settle.

The ransomware risk is not limited to big enterprises with huge databases. In fact, cybercriminals have increasingly set their sights on small- to medium-size businesses (SMBs). One reason is many SMBs operate retail and service organizations that necessitate keeping sensitive customer information on hand, such as personal credentials and financial records.

Another reason SMBs are targeted is they typically have fewer funds and employees available for deflecting ransomware than their larger corporate counterparts. That’s why as a top-tier managed services provider (MSP) we offer co-managed IT services such as remote management and monitoring that help defend against ransomware and other threats.

We can augment your internal cybersecurity team and more. Give us a call.

The Logical Advantage

Viewpoint

People: Your Best Cybersecurity Solution

Studies by Stanford confirm that nearly nine of every 10 data breaches result from human error.

But that doesn't mean you should treat humans as the weakest links in your company's chain of cybersecurity defenses. To the contrary, the best approach is to view people as your most valuable cybersecurity resource.

Here are three suggestions for better engaging your frontline team in fighting cybercrime:

1. Stop Blaming, Start Educating
Rather than admonishing workers for their mistakes, teach them how to recognize and avoid them in the first place. Tap into cybersecurity alert services. Launch awareness campaigns that provide recent examples of business email compromise (BEC)—in other words, the latest phishing techniques and other email scams. Develop practice scenarios and run preparation drills.

2. Track Behavioral Metrics
Yes, you should know how often your systems suffer assaults and how fast cybercrooks can penetrate your network perimeter. (Answers: Between 40-50 attacks if you run an average U.S. business and typically five hours for hackers to successfully crack your IT environment.) But you also should know how individual behaviors put your whole organization at risk and how changing those habits reduces the bad actors' success rates.

3. Engage Expert Support
As a top-tier IT managed services provider (MSP), we offer more than technical acumen. We share insights accumulated from assisting clients across an array of industries. How can we apply this knowledge to your business?

IT Strategy

3 Keys to Virtual Collaboration

Surveys show that SMBs plan to continue investing in collaboration solutions in 2023 as a technology priority, with budgets in this category growing as much as 10%.

During the last two years, social distancing protocols necessitated that companies of all sizes upgrade virtual collaboration tools, such as video conferencing platforms like Teams or Zoom. Now, spending will focus on IT investments that drive organizational transformation and business growth.

SMBs are no exception to this trend, with many seeking out partners who can provide strategic IT guidance to help them grow their businesses and increase revenue.

In that spirit, we offer three tips for effective virtual collaboration:

1. Keep Investing
Keeping your team's collaboration tools up to date with the latest upgrades and updates to productivity features is key to high ROI.

2. Set Routines, Adapt Often
Every department in your organization may have differing needs, requiring different configurations of collaboration tools. Each project team may need customized processes for scheduling or documentation. Make sure to proactively address needs and regularly revisit them.

3. Make Conversations Multichannel
Collaboration platforms integrate audio, video, email and text/chat formats for good reason. No need to use every channel every time, but definitely consider why, when and how you would use these various channels to communicate your messages.

If you need technical expertise evaluating, installing or maintaining collaboration solutions, let us know. We want to help you do business better.