Five emerging cybersecurity threats you should take very seriously

Five emerging cybersecurity threats you should take very seriously

Ransomware isn't the only cyberthreat your business will face this year. Here are five emerging threats that leaders need to know about.

The cyberthreat landscape continues to evolve, with new threats emerging almost daily. The ability to track and prepare to face these threats can help security and risk management leaders improve their organization's resilience and better support business goals.

The number of high-profile breaches and attacks making headlines has led business leaders to finally take cybersecurity seriously, said Sam Olyaei, senior principal and analyst at Gartner.

"Today, not only are business leaders and the business community understanding cybersecurity, they know it's important to their business outcomes and objectives," Olyaei said. "The problem is, there is still a lack of understanding as to why it's important."

Firms must work to bridge the gap between communicating the technical aspects of cybersecurity and the business outcomes, such as customer satisfaction, financial health, and reputation, Olyaei said.

Keeping track of new threats and not just established ones like ransomware is key for a strong security posture, said Josh Zelonis, senior analyst at Forrester.

"Whenever we develop our strategies for how we're going to protect our organizations, it's really easy to look at things that you're familiar with, or that you have a good understanding of," Zelonis said. "But if you're not looking ahead, you're building for the problems that already exist, and not setting yourself up for long-term success. And that is really the number one reason why you need to be looking ahead -- to understand how attack techniques are evolving."

Here are five emerging cybersecurity threats that business, technology, and security leaders need to take seriously this year.

1. Cryptojacking

Ransomware has been one of the biggest threats impacting businesses in the past two years, exploiting basic vulnerabilities including lack of network segmentation and backups, Gartner's Olyaei said.

Today, threat actors are employing the same variants of ransomware previously used to encrypt data to ransom an organization's resources or systems to mine for cryptocurrency -- a practice known as cryptojacking or cryptomining.

"These are strains of malware that are very similar to strains that different types of ransomware, like Petya and NotPetya, had in place, but instead it's kind of running in the background silently mining for cryptocurrency," Olyaei said.

The rise of cryptojacking means the argument that many SMB leaders used in the past -- that their business was too small to be attacked -- goes out the window, Olyaei said. "You still have computers, you still have resources, you still have applications," he added. "And these application systems, computers,

and resources can be used to mine for cryptocurrency. That's one of the biggest threats that we see from that standpoint."

2. Internet of Things (IoT) device threats

Companies are adding more and more devices to their infrastructures, said Forrester's Zelonis. "Organizations are going and adding solutions like security cameras and smart container ships, and a lot of these devices don't have how you're going to manage them factored into the design of the products."

Maintenance is often the last consideration when it comes to IoT, Zelonis said. Organizations that want to stay safe should require that all IoT devices be manageable and implement a process for updating them.

3. Geopolitical risks

More organizations are starting to consider where their products are based or implemented and where their data is stored, in terms of cybersecurity risks and regulations, Olyaei said.

"When you have regulations like GDPR and threat actors that emerge from nation states like Russia, China, North Korea, and Iran, more and more organizations are beginning to evaluate the intricacies of the security controls of their vendors and their suppliers," Olyaei said. "They're looking at geopolitical risk as a cyber risk, whereas in the past geopolitical was sort of a separate risk function, belonging in enterprise risk."

If organizations do not consider location and geopolitical risk, those that store data in a third party or a nation state that is very sensitive will run the risk of threat actors or nation state resources being used against them, Olyaei said. "If you do that then you also impact the business outcome."

4. Cross-site scripting

Organizations struggle to avoid cross-site scripting (XSS) attacks in the development cycle, Zelonis said. More than 21 percent of vulnerabilities identified by bug bounty programs are XSS areas, making them the leading vulnerability type, Forrester research found.

XSS attacks allow adversaries to use business websites to execute untrusted code in a victim's browser, making it easy for a criminal to interact with a user and steal their cookie information used for authentication to hijack the site without any credentials, Forrester said.

Security teams often discount the severity of this attack, Zelonis said. But bug bounty programs can help identify XSS attacks and other weaknesses in your systems, he added.

5. Mobile malware

Mobile devices are increasingly a top attack target -- a trend rooted in poor vulnerability management, according to Forrester. But the analyst firm said many organizations that try to deploy mobile device management (MDM) solutions find that privacy concerns limit adoption.

The biggest pain point in this space is the Android installed base, Zelonis said. "The Google developer site shows that the vast majority of Android devices in the world are running pretty old versions of Android," he said. "And when you look at the motivations of a lot of IoT device manufacturers, it's challenging to get them to continue to support devices and get timely patches, because then you're getting back to mobile issues."

Organizations should ensure employee access to an anti-malware solution, Forrester recommended. Even if it's not managed by the organization, this will alleviate some security concerns.