COMCAST BUSINESS | MASERGY

WHAT YOU'LL LEARN

- Which threats are most costly
- Cloud and SaaS security risks
- How AI is driving cybercrime

E - GUIDE

The top 5 cybersecurity threats to watch out for now

The threat landscape is constantly evolving. Thus, it's crucial for companies and all privacy-minded users to heighten their awareness around the latest cybersecurity threats. In 2019, every organization should be prepared for these top five security threats.

1. Ransomware & malware: more costly than data breaches

Ransomware is already on track to hit $11.5B in damages for 2019, which roughly translates into someone becoming a new victim every 14 seconds. Using malware or software to deny access to a computer or system until a ransom is paid, these threats are more costly than traditional data breaches alone. But ironically, it's not the threat of paying a ransom and the cost of stolen data that's proding executives to heighten their security protections. These days, the motivating factor is minimizing the most expensive impact--the broader organizational disruption of a cyber attack and the cost to both clean up the network and restore business operations. Ransomware is on the rise, and it will cost more than you might think.

2. Endpoint attacks: cloud and SaaS trends make it easier for hackers

As companies move more and more resources into the “cloud”, attack surfaces will continue to grow in size, thus making it easier for intruders to get past security measures. With the bring-your-own-device culture that we live in today combined with the proliferation of SaaS providers for data services, hackers have plenty of attack vectors from which to choose.

The challenge that organizations face today is securing access into these off-premise resources, which are commonly used as stepping stones for bad actors to get into your network. After all, every attack begins at the endpoint, whether it serves as the true target or not. So, whether the risk comes from the unauthorized use of Shadow IT applications co-mingled with company resources or users simply getting “pwned” (hacked) off the corporate network through other means, the threat to the user endpoint is a real challenge that has yet to be solved.

3. Phishing: more sophisticated than ever

Phishing has long been proven to be one of the cheapest and easiest ways to compromise targets, which is why it remains the #1 cyber attack vector for hackers. More often than not, phishing attacks appear to be normal, everyday emails from trusted sources but deliver malware to your computer or device, giving the hacker the critical access they need.

With the widespread use of SaaS services like Dropbox, Slack, Office 365, Salesforce and others, hackers are improving their impersonation skills with more sophisticated attack types ranging from credential stuffing to advanced social engineering methodologies. The content is becoming more relevant and interesting to potential victims, luring them to engage and divulge information. As a result, these attacks have become more difficult to recognize, even for tech-savvy users.

4. Third party & supply chain attacks: on the rise

A supply chain attack (also called a third-party attack) occurs when your system gets infiltrated through an outside partner or provider that has access to your systems and/or data. With more digital supply chains and service providers touching more enterprise data than ever before, the attack surface has dramatically changed. Hackers have wider opportunities, and these types of attacks are becoming more apparent.

Software updates and security patches are critical protections, yet another area of vulnerability when working with third parties. Most third-party software is dependent on external libraries and resources for updates and patches. If these external resources are compromised by bad actors, they can easily redirect system updates to malicious servers to deliver malware to their victims.

5. AI- and ML-driven attacks: cybercrime evolves with advanced tools

Machine Learning (ML) and other Artificial Intelligence (AI) approaches are now being used to fight cyber crime, becoming “table stakes” in all modern security strategies. But the same tools are being used against us.

As ML and AI become more readily available to the masses, hackers are using them to enhance the sophistication of their attacks. With these tools, attacks can be multiplied and cybercrime can reach all-new heights. We’re already seeing the evidence! Many of the recent widespread ransomware attacks are ML- and AI-driven.

Additional resources

- Build or Buy? Eight Factors for Measuring TCO on Security Operations Center
- There’s Help for CISOs Overwhelmed By Security Threats
- The Truths and Lies of IoT Security: Monitoring Connected Devices
- SD-WAN Security Guide: Broadband, Bundled Features, and Buyer Tips
- How To Secure IaaS/PaaS Effectively: Customer Responsibilities in the Shared Security Model

About Masergy

Masergy is the software-defined network and cloud platform for the digital enterprise. Recognized as the pioneer in software-defined networking, Masergy enables unrivaled application performance across the network and the cloud with Managed SD-WAN, UCaaS, CCaaS, and Managed Security solutions. Industry-leading SLAs coupled with an unparalleled customer experience enable global enterprises to achieve business outcomes with certainty.