THE TECH WALK
5/8/22

FIVE TRENDS IN CYBER SECURITY THREATS

Cyber security is a fast-paced industry in which hackers and security providers compete to outwit one another. New threats — and inventive strategies to address them – develop on a regular basis. In this review, we will look at the most recent cyber security developments.

1. Ransomware - The Rise:

Ransomware isn't a new danger; it's been around for over two decades, but it's becoming more prevalent. It is claimed that there are now over 120 distinct kinds of ransomware, and hackers have gotten quite skilled at concealing dangerous code. Ransomware is a very simple means for hackers to receive money incentives, which contributes to its popularity. The Covid-19 epidemic was another issue. Many firms' increasing digitalization, along with remote working, generated new targets for ransomware. As a result, both the number of attacks and the magnitude of demands grew.

Extortion attacks entail thieves taking a company's data and encrypting it so that it cannot be accessed. Following that, fraudsters threaten to reveal the organization's sensitive data unless a ransom is paid. Given the sensitive data at stake, as well as the economic consequence of paying the ransom, the cost of this cyberthreat is enormous.

In 2020, ransomware made history by being a factor in the first documented fatality caused by a cyber-attack. In this case, a hospital in Germany was shut out of its systems, preventing it from treating patients. A woman in need of immediate medical attention was sent to a nearby hospital 20 miles away, but she did not survive.

Through machine learning and more coordinated sharing on the dark web, ransomware criminals are getting more adept in their phishing operations. Hackers frequently demand payment in cryptocurrencies that are tough to track down. In the near future, we should expect to see more ransomware assaults on enterprises that are not cyber safe.

2. Increase in Cloud services and cloud security concerns.

Cloud vulnerability is one of the most significant cyber security industry trends. Again, the pandemic's quick and broad adoption of remote working boosted the need for cloud-based services and infrastructure dramatically, with security issues for enterprises.

Cloud services have several advantages, including scalability, efficiency, and cost savings. They are, nevertheless, a prime target for attackers. Misconfigured cloud settings are a major source of data breaches and illegal access, as well as insecure interfaces and account hijacking. Because the average cost of a data breach is $3.86 million, enterprises must take precautions to reduce cloud vulnerabilities.

Aside from data breaches, enterprises face the following network security trends and cloud security challenges:

a. Ensure cross-jurisdictional regulatory compliance

b. Providing adequate IT knowledge to meet the expectations of cloud computing

c. Problems with cloud migration

d. Managing additional possible access points for attackers

e. Insider risks, both unintentional and purposeful, are caused by unauthorised remote access, weak passwords, insecure networks, and personal device usage.

3. More sophisticated Social Engineering Assaults

Social engineering assaults, like as phishing, are not new risks, but they have become more concerning in light of the increasing remote workforce. Individuals connecting to their employer's network from home are easier targets for attackers. In addition to standard phishing attacks on employees, there has been an increase in whaling assaults against upper organisational leadership.

SMS phishing, often known as 'smishing' is growing popularity as a result of the popularity of messaging programmes such as WhatsApp, Slack, Skype, Signal, WeChat, and others. These sites are used by attackers to lure consumers into installing malware onto their phones.

Another kind is voice phishing, sometimes known as 'vishing,' which gained popularity in a 2020 Twitter attack. Hackers impersonating IT personnel phoned customer support reps and duped them into granting access to a critical internal tool.

SIM jacking occurs when fraudsters call personnel of a client's cell network and convince them that their SIM card has been hijacked. As a result, the phone number must be transferred to another card. If the deception is effective, the cybercriminal has access to the target's phone's digital contents.

Organizations are beefing up their anti-phishing defences, but thieves are continuously seeking for new methods to stay ahead. This includes sophisticated phishing kits that target victims differently based on where they are.

4. Artificial intelligence's continued ascent (AI)

Humans are incapable of dealing with the sheer amount of cyber security threats. As a result, enterprises are increasingly relying on artificial intelligence and machine learning to improve their security architecture. There are financial savings to doing so: firms who experienced a data breach but fully adopted AI technology saved an average of $3.58 million in 2020.

AI has played a critical role in the development of automated security systems, natural language processing, facial identification, and autonomous threat detection. AI also allows for the analysis of enormous amounts of risk data at a much faster rate. This is advantageous for both huge corporations dealing with massive volumes of data and small or medium-sized businesses with under-resourced security teams.

While AI offers organisations a big possibility for more powerful threat detection, criminals are also leveraging the technology to automate their assaults through data-poisoning and model-stealing approaches.

The practical uses of AI are constantly evolving; we expect security systems powered by AI and machine learning to become more sophisticated and capable.

5. Mobile cybersecurity is gaining prominence.

The move toward remote working is also hastening mobile's rise. It is common for remote employees to move between a variety of mobile devices, such as tablets and phones, while using public Wi-Fi networks and remote collaboration applications. As a result, mobile risks are growing and evolving. The continued spread of 5G technology generates possible security flaws, which must be corrected as they emerge.

Mobile risks include the following:

Spyware created specifically to snoop on encrypted chat applications.

Criminals are taking advantage of serious security flaws in Android smartphones.

Mobile malware offers a wide range of conceivable application scenarios, including DDoS attacks, SMS spam, and data theft.

Mobile cybersecurity is a wide problem that includes back-end/cloud security, network security, and a network of increasingly linked items (i.e., the Internet of Things), such as wearables and automobile gadgets. There is no one approach for protecting apps in unsafe settings; rather, it is about adding extra layers of protection to boost overall security. To strengthen sensitive data storage, security experts are integrating mobile software security with hardware-based security solutions.

Cybercriminals are continuously seeking for new methods to attack and harm individuals and businesses in this age of accelerating digital change, which means cybersecurity challenges are evolving. Using a good antivirus software solution does the job pretty well, in securing your systems among these cyber threats!

Thanks for Reading!

Stay subscribed to The Tech Walk for a regular walkthrough of technology and trends flying around.