Cybersecurity Trends Unveiled: What You Need to Know

By Shikha Mehta

Unpacking Cybersecurity for the Modern World

The number of digital devices in use has increased dramatically over the last ten years of technological advancement, and it continues to rise even today. But as the number of digital devices rises, so does the burden of defending them from outside influence. In the modern world, Cybersecurity entails safeguarding essential technological assets of an individual or an organization and establishing a secure online environment to keep the threat actors out. It is an evolving technology with a wide range of domains as well as many uncharted territories.

Today, Cybersecurity has orchestrated an enormous wave of trends and technologies that go beyond what we know so far. It has been able to break through the shackles of traditional boundaries of the digital landscape and produce a secure cyberspace for our digital assets. It involves protecting data from unauthorized access, adhering to compliance standards, and promoting a cyber-resilient infrastructure in businesses. Data Privacy has garnered a lot of importance in security since high-profile data breaches affecting millions of people have increased alarmingly. To prevent misuse of this data, compliance requirements are followed to uphold these data privacy standards. These laws are created to protect the sensitive consumer info that's so often stolen in these security breaches. Compliances such as HIPAA and PCI-DSS are extensively used in the healthcare and financial industry respectively.

In this blog, we explore some of the latest cybersecurity trends that have emerged and their effects on the overall digital infrastructure. These trends include the use of AI in Cybersecurity, Zero Trust Security Models, Blockchain Security, and the increase in Ransomware Attacks. But before that, let's unmask the dangers lurking in cyberspace: Malware.

Malware Decoded: How to Recognize and Combat Online Threats

Any malicious program intended to disrupt systems, networks, and devices is referred to as malware, or malicious software. Without the proper authorization, malware can infiltrate your system and be used to steal confidential customer data, compromise data, lock you out of the device until you pay a ransom, or flood targets with spam from an infected machine. Malware can be added to emails as attachments and is initially introduced into the system through social engineering strategies like phishing. The attacker can spy on and harm systems after the victim

downloads the attachment, giving them unauthorized access to the network. After that, not only does the malware slow down the speed of the internet and other software applications but may also cause machine crashes during normal use.

There are different types of Malwares that may be used to gain access to your system:

1. **Viruses:** Viruses are malicious codes hidden in executable files and wait for the victim to execute it. Just like an actual virus, a computer virus also needs to be replicated and spread to different systems by a host system. Viruses can affect the working of the target system by corrupting it.

2. **Worms:** Unlike a Virus, a Worm doesn't require a host to replicate itself. Their primary goal is to use up system resources, which causes the computer system to operate at a slower pace. Worms connect to numerous machines in order to propagate throughout the network.

3. **Trojans:** This type of malware appears to be legitimate software and is accepted into the system easily. It, then, creates backdoors for remote access at a later time.

4. **Ransomware:** Ransomware encrypts an organization's private information, demands a ransom to unlock it, or threatens to sell or leak the information to the dark web.

5. **Spyware:** A spyware discreetly keeps an eye on the victim's computer. It gathers data while disguising itself as a background application without the user's awareness.

6. **Adware:** This type of malware automatically displays or downloads unwanted advertisements and generates revenue for it. Because it tracks user behavior, this malware may potentially compromise security in addition to frequently annoying users.

7. **Rootkits:** A Rootkit allows an attacker to have remote administrator privileges, while remaining hidden from users or system administrators.

Cybercriminals used the notorious CovidLock ransomware of 2020 for their own illicit gains. On an Android device, this ransomware encrypted important data and prevented its victims from accessing it until they paid a ransom. The victim's contact information and other data were held hostage by the app, which demanded ransom in exchange for access to the coronavirus map tracker. Another such incident was the WannaCry ransomware attack that occurred on May 12, 2017.It disseminated via the use of the "EternalBlue" vulnerability exploit. Only unpatched versions of Microsoft Windows were compatible with EternalBlue, but there were plenty of

machines running these versions to facilitate WannaCry's quick spread. In 150 countries, it affected over 200,000 computers.

Considering the significance of these occurrences, it is critical to keep an eye out for potentially harmful websites, pop-up ads, and spam emails on your devices in order to defend against malware attacks. When clicking links from unfamiliar sources, exercise caution as they might be phishing attempts. Backing up data can be helpful in the event of a malware attack where data can be easily restored. Sandboxing can be used to isolate malware to a protected environment. Firewalls can be deployed to filter out suspicious network traffic. Finally, keeping your anti-malware tools up-to-date can help battle against any malware that may have been accidentally introduced in the system.

Breaking Down Complex Cybersecurity Trends

AI in Cybersecurity

The increasing frequency, complexity, and speed of cyber threats is a result of artificial intelligence (AI) which makes it important to understand AI's role in cybersecurity. With the use of AI, cyber threat actors have evolved, making their attacks increasingly sophisticated. In fact, artificial intelligence operates at the speed of a machine and is imperceptible to traditional security measures. Thus, in order to defeat these attackers at their own game, we also started implementing AI-driven detection and analysis. Predictive AI was first introduced to forecast threats. It was later expanded by adding User and Entity Behavior Analytics (UEBA) which focuses on user behavior patterns. It has now grown even further with the use of Generative AI (GenAI). The AI-based components that we use are Machine Learning, Natural Language Processing, Data Mining, Predictive Analysis, Behavioral Analytics, and Automated Decision Making. Artificial intelligence (AI) provides an unparalleled degree of efficiency and continuous learning that can enhance human capabilities. AI is ,therefore, used for threat hunting, threat detection, and response and mitigation efforts.

Zero Trust Security Models

In a traditional security infrastructure, it is hard to gain access to a system from outside. However, once you have successfully authenticated, the system assumes you are trustworthy. This causes a problem since an attacker may get free reign over everything inside the system. Furthermore, it is impossible to have a single security control over the entire network because data is not stored in a single location. Hence, Zero Trust Security Model is adopted. It works on the principle that no one is trusted by default from inside or outside of the network. This implies that even if the user is already logged in, verification is still necessary in order to use the resources. This added layer of security does a great job in preventing security breaches. Zero

Trust can be used when on-boarding third-parties and contractors or new employees and can also be used for access control for cloud and multi-cloud purposes.

Rise of Ransomware Attacks

Ransomware is a type of malware that holds the data hostage by encrypting it and demands a ransom in return to decrypt it. This attack has grown in popularity and complexity, especially in the last decade, making it harder to crack the encrypted data. It is now more difficult to unlock the files without paying the ransom because the stakes for the victims have increased as well. Hackers may even "dwell" or embed inside an organization's computer system undetected for weeks or months to gain access to the most valuable data of the organization. These hackers then often threaten to sell or leak data. As a result, the business may not only suffer from financial loss but also from reputation loss. Consumers are reluctant to put their trust in that company, and an increasing number of attackers are motivated to carry out similar attacks in the future. These attacks have seen a drastic increase both in number and in scope. The fact that more businesses are opting to pay the ransom in order to recover their data is the main cause of the surge in these attacks, and cybercriminals are taking notice. Ransomware attacks can be controlled by dealing with them proactively rather than reactively. Getting assistance from law enforcement is another valid solution to this crisis.

Blockchain

Blockchain is an online cryptosystem of recording information using Distributed Ledger Technology that makes it difficult or impossible to change, hack, or cheat the system. Blockchain security relies on 'one-way' mathematical functions. These are straightforward to run on a conventional computer and difficult to calculate in reverse. A blockchain is a chain of blocks that adds a new block whenever a transaction is requested and authenticated. However, this system is vulnerable to the advances in quantum technology (because traditional computer parts are now approaching the size of atoms) and might not be able to protect itself against the future threats posed by large-scale quantum computers. Therefore, there is a need for post-quantum cryptography that would be impenetrable not only to future quantum attacks but also to classical attacks right now.

Protecting Your Business from Cyber Attacks

Businesses often work with critical data that need to be available round the clock with zero downtime for smooth business operations. Threat vectors such as internal threats, competitive threats, and zero-day attacks can pose a risk to a business. These security flaws could interfere with business operations and result in loss of both money and reputation. Therefore, the actions listed below can be implemented to defend businesses against cybersecurity risks:

- Limited employee access to data and information to reduce human error

- Deploying Uninterruptible Power Supplies to recover from short-term power loss
- Patching operating systems and software regularly to eliminate security vulnerabilities
- Deploying Hardware and Software Firewalls to stop employees from visiting dangerous sites
- Setting up Web and EMail Filters to prevent spam flooding in employee inboxes
- Using encryption to protect sensitive information from threat actors
- Training employees on cybersecurity incident response and proper handling of company data both at work and at home.

Cyber Protection Checklist: Must-Do Tips

Promoting best practices for cybersecurity is the need of the hour. This can be done via a checklist that provides essential procedures to protect against changing cyberthreats and is crucial for security of personal devices as well as corporate networks. The following items are on this checklist:

- Data should be encrypted at rest, in use, or in motion.
- A Disaster Recovery Policy should be in place in the event of an unforeseen cybersecurity incident.
- Update Software frequently to patch known vulnerabilities in time
- Cybersecurity Insurance is a useful way of risk transference to protect against financial losses from cybersecurity incidents
- Keeping Anti-Malware signature database up-to-date by updating it regularly.
- Least Privilege Access principle must be followed to limit user access based on their roles
- Providing Cybersecurity Training to employees and prepare them for incident response

Cybersecurity Roundup: Key Takeaways

In an age where the use of digital devices is growing quickly and sophisticated cyber threats prevail, businesses need to take a proactive approach to cybersecurity. Getting cyber insurance is one of the most important tactics to reduce the financial damage caused by attacks, especially ransomware, which is becoming more and more common. Strong security measures for remote access and thorough employee training are required in light of the growing popularity of remote work in order to thwart phishing and other social engineering attacks.

Artificial intelligence is essential for improving cybersecurity because it can identify threats in real time and trigger automated responses. To find and fix possible vulnerabilities, regular risk assessments and indispensable tools like firewalls, antivirus software, and encryption are required. Adopting a Zero Trust Security Model guarantees that there is no implicit trust in

networks, and in spite of its vulnerability to quantum computing, blockchain technology presents promising security solutions. Adopting best practices, such as restricting employee access to data, updating systems frequently, and organizing proactive incident response plans, is another aspect of safeguarding a company. Businesses can build a resilient cybersecurity infrastructure that can fend off changing threats by being vigilant and implementing these precautions.