International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 12 | Dec 2022 www.irjet.net p-ISSN: 2395-0072

Latest Cybersecurity Trends

Kajal Kadam[1], Aliya Shaikh[2], Asst.Prof. P.S.Gade[3]

[1]Kajal Kadam, YTC, Satara, Maharastra India
[2]Aliya Shaikh, YTC, Satara Maharastra India
[3]Asst.Prof.P.S.Gade,YTC, Satara, Maharastra India

Abstract - *The likelihood of a security breach has never been higher due to the variety of new threats that are developing from both inside and outside your network. The combination of all these risk variables with a significant human component presupposes that everything has been set up and configured correctly to get the best results possible from each security instrument. In order to address this issue, organisations often spend more money on security controls, which increases management visibility and makes it easier for team like Security operation to see better results and provide good return on investment.*

The author covers the current trends in cybersecurity in this research report. Investigations have also focused on cybersecurity trends advantages and potential growth. The conceptual analysis of trends as a whole in the research has also given consideration to future evolution.

Key Words: Cyber Security, Data, Attacks, Threats, Cryptocurrency, Breach

1. INTRODUCTION

The cyber security domain growing faster as both offensive and defensive security service providers compete to outwit one another. Technology is constantly developing and improving, and new threats and creative solutions to combat them are constantly emerging. As more people started working from home recently due to the pandemic, fraudsters discovered new techniques, tactics, and strategies to take over networks and steal data in order to exact a ransom.

The newest developments in cyber security are discussed in this overview.

2. CYBER SECURITY TRENDS

2.1 Machine Learning

Although it is one of the newest technologies in cybersecurity, machine learning is playing a bigger and more proactive role. One of the reasons is that machine learning makes cybersecurity easier, more efficient, and less expensive (ML). This system builds patterns and manipulates them, anticipating and responding to active attacks in real-time using sophisticated algorithms that are based on complex data. To put it another way, applying ML to cybersecurity systems helps them to assess threat patterns and learn the habits of hackers, assisting in the prevention of future attacks and decreasing the amount of time cybersecurity experts must dedicate to repetitive operations.

ML makes cybersecurity easier to use, more efficient, and more affordable all at once. ML creates patterns and uses algorithms to alter them from a complex set of data. It can therefore anticipate dangers in real time and respond to them accordingly. In order to create efficient algorithms, this technology primarily depends on complex and rich data. The information must come from everywhere and must cover as many probable outcomes as is practical. In order to assess attack trends and learn hackers' tactics, cybersecurity systems can now use machine learning (ML)

2.2. Artificial Intelligence (AI)

It is impossible for human being to operate large number of cyber security threats. As a result, organisations are increasingly turning to AI and ML to hone their security infrastructure. Al has played a key role in developing automatic threat detection, face recognition, natural language processing, and security automation systems. Al also enables the much quicker analysis of enormous amounts of danger data. This is advantageous for both huge enterprises dealing with massive amounts of data and small or mid-sized businesses with sometimes under-resourced security teams. While Al has enormous potential for businesses to detect threats more thoroughly, thieves are also leveraging the technology to automate their attacks by using model-stealing and data-poisoning methods.

2.3 Need of Multi-Factor Authentication

Password protection is no longer enough due to the sophistication of modern cyberattacks. Compared to a basic password, a multi-factor authentication (MFA) is much more secure. By simply adding an additional layer of security, multi-factor authentication helps to prevent illegal access to online accounts. MFA makes sure that businesses can better safeguard employee data and manage access. Every time someone signs in, they must additionally provide a verification code that is sent to their registered phone number or through an authenticator app. The "gold standard" of authentication is multi-factor authentication (MFA).

In order to solve this problem, organisations will increasingly use on application-based MFA tools like Microsoft Authenticator, Google Authenticator, One Span Authenticator, and others. Despite this, because SMS and voice MFAs are not end-to-end encrypted, they are still susceptible to attacks. Microsoft also suggested their customers to use app-based authenticator with the keys instead of phone-based authenticator. Despite this SMS and voice MFA continue to be vulnerable as these channels are not encrypted.

2.4 Rise of Ransomware

Even though ransomware has been a threat for over 20 years, it is still becoming worse. The frequency of ransomware cyberattacks is considered to have significantly grown now a days. In this cyberattack attacker finds access to the sensitive data of a person, a group, or a organization and then encrypt it so they cannot access it. They then convey a threat to reveal personal information if a ransom is not paid, which is typically made in bitcoin.

The burden of this cyber threat is significant given the sensitive data at stake as well economic impact of paying the Ransome. Remote working and the growing digitization of many enterprises have given ransomware new targets.

As the number of attacks is increased, the quantity of Ransome paid is also increased. Most of the time, hackers demand such payments in obscure cryptocurrency.

5. Breach and Attack Simulation (BAS)

In the last two decades, cyberattacks have undergone a significant evolution in terms of their capabilities, reach, consequences, and variety of targets. Cybercrime is causing record-breaking losses worldwide, and it appears that this trend will continue. Security managers and executives are aiming to improve their company's security posture because of the increased danger of attacks. BAS technologies are described as technology "that enable enterprises to continuously and consistently simulate the full attack cycle against enterprise infrastructure, using software agents, virtual machines, and other means, including insider threats, lateral movement, and data exfiltration."

The uniqueness of BAS resides in its capability to deliver consistent and reliable simulation assessment with minimal risk, as well as its use in warning IT and business stakeholders about existing security posture gaps or confirming that security infrastructure, configuration settings, and detection technologies are functioning as intended. When utilised in addition to red team or penetration testing assessment, BAS can help validate to identify whether security operations and the SOC staff can detect certain cyberattacks.

2.6. Cloud Security

More and more businesses are moving to the cloud as a result of the significant benefits it provides. To combat online criminals, a cutting-edge predictive security model must be used if the cloud is to be secure. Attacks on cloud services have grown over the past ten years, making them a risky way to store or transfer sensitive data. Secure encryption, authentication, and audit logging are not typically provided by cloud services. Others do not properly separate user data from that of other cloud tenants who share the same space. Security experts believe that cloud security needs to be strengthened as a result.

Threats can now be detected by predictive security before an attacker even makes a move. It has the ability to identify attacks that get past other endpoint security. In order to strengthen security, businesses are implementing predictive security clouds, and some industries have also turned to multi-factor authentication.

Although cloud computing has many advantages, including cost-effectiveness, scalability, and efficiency, it also has drawbacks that cannot be avoided. They are a top target for attackers as well. Insecure interfaces, account theft, and data breaches are all frequently brought on by improperly configured cloud settings.

2.7 IOT

The Internet of Things (loT) has completely changed the way we interact with devices. Despite some security issues with loT devices, which are common, most consumers have a high level of confidence in them. loT devices are currently dominating the consumer markets. Smart gadgets, air conditioning with built-in intelligence, wearable fitness trackers, and voice assistants like Google Home and Amazon Echo are a few examples of loT devices. Despite the fact that loT provide more convenience, they also pose greater risks to a user's data. In the event that a device is compromised or taken over, it could essentially act as a listening device and steal data from the network.

Hackers have discovered a new entry point for information and are making the most of it. To gain access to security systems, for instance, hackers frequently attempt to hack into connected camera networks or devices. If proper security measures aren't taken, the network is also exposed to software bugs or vulnerabilities by the communication protocols used to connect with various devices, increasing the possibility of outbreaks.

3. ADVANTAGES

- Unauthorized access to data and network is protected.

- Early detection of threats and vulnerabilities.
- Protection from cyber-attacks/breaches.

4. CONCLUSION

With new and complex risks emerging every day, the cyberworld is continually evolving. Although most people think they are protected from cyber threats, almost everyone is actually vulnerable. There are always new strategies to defend your firm against these threats as new trends emerge. Keeping an eye out for any new cybersecurity trends you can ensure the security of your organisation. There are numerous new trends that you need carefully investigate in order to choose the one that best suits your demands.

REFERENCES

- CISSP: Certified Information Systems Security Professional Study Guide (Sybex)
- Isc2 Cissp Certified Information Systems Security Professional Official Study Guide