ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 05/23 (May)

Top Cybersecurity Trends for 2023: Best Practices & Recommended Measures to Prevent Cyber Attacks

OVERVIEW

With the increase in remote work and cloud usage as well as Artificial Intelligence (AI) and Internet of Things (IoT) applications, the world is expected to spend more on cyber security and risk management in 2023 compared to 2022. For instance, an International Data Corporation forecast predicted a 12.1% increase in global spending on security solutions, including in endpoint security and cybersecurity policy compliance, between 2022 and 2023.

TOP CYBERSECURITY TRENDS FOR 2023

Several trends perpetuate the attack surface, including the hybrid work environment and the shift to cloud. Here are some of the top cybersecurity trends to keep an eye on:

1. Remote workforce security

The remote work trend will continue in 2023 and beyond. Remote environments are harder to secure, as they lie outside organisational perimeters. Apart from working from home, workers may access their IT devices from anywhere, such as malls or cafes, where public wifi may be used. Such hybrid work environments are a source of risk, as they expand the area of potential cyberattacks. To ensure secure remote and hybrid work, organisations should implement strong security protocols such as VPNs, multi-factor authentication, and endpoint/mobile device security solutions. They should also educate employees on identifying risks and cybersecurity practices, as well as maintaining strong password hygiene.

2. Cloud security

Shifting to the cloud brings great opportunities, cost savings and convenience. However, securing cloud infrastructure may be challenging due to the increased number of attack vectors, the complexity of cloud environments, and the sharing of security responsibilities between the client and the cloud services provider. To ensure cloud security, the cloud provider is responsible for securing the infrastructure, access, patching and configuration of hosts/networks, while the customer needs to manage users and access privileges, protect cloud accounts, encrypt/protect data and maintaining compliance.

3. Mobile security

The mobile phone has replaced our trips to the banks, supermarkets and physical stores. With just a few taps on our phones or laptops, there is no need to leave the comfort of our homes to get what we want. While this has led to greater convenience to our everyday lives, malicious actors will exploit every opportunity in e-commerce, banking services, and online bookings to carry out malicious and unauthorised activities on the device. Ensuring that our mobile devices are updated regularly and not installing applications from untrusted origins is crucial to guard against cyber attacks.

4. Supply chain security

In today's interconnected world, supply chains rely heavily on information systems, digital technologies and communication networks. Cyber security and defence is critical, to protect sensitive data and proprietary information; prevent data breaches; ransomware attacks and phishing attempts; and prevent disruptions to operations such as delivery of goods and services. Identifying and mitigating risks can be done through a combination of risk management, cyber defence, adherence to relevant government protocols and incident response plans.

5. AI and Machine Learning (ML)

As AI and ML technologies become more advanced and prevalent, they also become more attractive to cybercriminals and adversaries. Attackers could automate and scale their malicious activities such as generating AI-powered deepfakes for malicious intent and AI-supported malware for hacking. In addition, with the growing use of AI chatbots such as ChatGPT, users must be vigilant when sharing them as these tools rely on large amounts of input to generate data and information. Attacks on AI chatbots can reveal sensitive or confidential information. However, when properly secured and monitored, AI and ML can also be used to improve cybersecurity defences and mitigate potential threats.

6. Information Technology (IT) / Operational Technology (OT) - IoT Convergence

The IT/OT-IoT convergence integrates data collection (IT) with control processes (OT-IoT). IT/OT-IoT convergence allows organisations to streamline and automate processes more efficiently. Security measures and protocols for IT and OT-IoT devices are still developing, which may open up opportunities for weaknesses that cyber attackers may exploit to gain footholds in organisations. Hence, organisations should prioritise securing vulnerable IT/OT-IoT devices to prevent cyber-attack incidents.

7. 5G security

5G technology is designed to provide greater network capacity and faster data transfer with significant improvements in speed, latency and bandwidth. 5G security protects high-speed mobile services for billions of devices and the IoT. However, the increase in the number of mobile services means an increase in attack vectors which threat actors can gain access to. Organisations should leverage on the existing 5G frameworks such as European Union's 5G Toolbox adopted in January 2020 to securely utilise 5G technology.

8. Blockchain security

Blockchain technology is an advanced database mechanism that allow transparent information sharing within a business network. It is an innovative technology that enable decentralised digital transformation. However, due to Blockchain's decentralisation and openness, its security becomes challenging. Blockchain security will require risk assessment, implementation of cybersecurity frameworks, security testing, and secure coding to protect against associated vulnerabilities.

9. Quantum computing

Quantum computing comprises aspects of computer science, physics and mathematics that utilises quantum mechanics to solve complex problems faster than on classical computers. Quantum computing may aid breakthroughs in many fields such as medical research, artificial intelligence and other fields of research that needs to compute copious amounts of data. However, quantum computing also threatens to break the traditional encryption methods used for secure data protection. To counter this, organisations should adopt quantum-resistant solutions now.

Knowing these cybersecurity trends in 2023 will allow the organisations to tailor their cybersecurity measures more accurately and effectively.

BEST PRACTICES AND RECOMMENDED MEASURES TO PREVENT CYBER-ATTACKS

Proactive cybersecurity reduces the impact of cyber-attacks. Below are some new and time proven cybersecurity principles and best practices for organisations to prevent cyber-attacks in 2023:

1. Establish a robust cybersecurity policy

A cybersecurity policy serves as an official guide to all measures used in your organisation to improve cybersecurity efficiency and is useful for everyone to be up-to-date with the company's security practices. Organisations could consider implementing a centralised cybersecurity policy with customised department policies. This will help organisations increase overall cybersecurity policy effectiveness and avoid disrupting departments' workflows.

2. Use multi-factor authentication (MFA)

Organisations are advised to secure remote access applications and enforce MFA on local/remote accounts and devices where possible to harden the infrastructure that enables access to networks and systems. This is especially so for environments where users perform privileged actions or access important (sensitive or high-availability) data repositories.

3. Manage passwords wisely

Employee credentials provide cybercriminals direct access to sensitive data and valuable information. Brute force attacks, social engineering, and other methods can be used to compromise employees' credentials without them knowing. Organisations should enforce a strong password security policy and/or specialised password management tools to prevent unauthorised access and thus mitigating such attacks.

4. Manage supply chain risks

An organisation's vendors, partners, subcontractors, suppliers, and other third-parties with access to organisational resources may be susceptible to supply chain attacks as they are potential attack vectors for a data breach or cyber attack to gain access into the organisation. One way to safeguard sensitive data is to monitor and limit what 3rd party users can do in the organisation's IT environment. To address supply chain risks, organisations need to develop a comprehensive strategy of cyber supply chain risk management to enhance business continuity and improve supply chain visibility.

5. Secure perimeter and IoT connections

Consider safeguarding your perimeter by setting up screened subnets and securing your border routers. Sensitive data from corporate networks should also be segregated with access restrictions to lower data security concerns.

6. Patch systems and applications in a timely manner

Enable automatic patching processes for all software and hardware devices where possible. Threat intelligence can be leveraged to identify active threats and protect exposed systems and infrastructure. Secure software assets through an asset management program that includes a product lifecycle process. This process should include planning replacements for components and software nearing or past end-of-life, as patches may cease to be developed by manufacturers or developers.

7. Protect and manage data

Data management policies provide clear guidelines for information management procedures. It also provides a framework for ensuring compliance with laws and regulations. This process can help to reduce data breaches and ensure cybersecurity regulations compliance.

CONCLUSION

To secure against evolving cyber threats and the ever increasing attack vectors, organisations in 2023 must continuously update their cybersecurity policies, review best practices and ensure employees are educated on cyber risks. Using a people-centric approach, employees and IT administrators can work together to reduce cyber occurrences and incidents.

Contact Details

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

ANNEX A

News Articles

1. Cybersecurity Best Practices & Measures to Prevent Cyber Attacks in 2023 [Link: https://www.ekransystem.com/en/blog/best-cyber-security-practices]

2. Cybersecurity Best Practices for Smart Cities | CISA [Link: https://www.cisa.gov/resources-tools/resources/ cybersecurity-best-practices-smart-cities]

3. Top 10 cybersecurity best practices to Prevent Cyber Attacks in 2023 [Link: https://www.analyticsinsight.net/top-10-cybersecurity-practices-to-prevent-cyber-attacks-in-2023/]

4. Securing The Future: The Most Critical Cybersecurity Trends Of 2023 [Link: https://www.forbes.com/sites/forbestechcouncil/2023/02/ 28/securing-the-future-the-most-critical-cybersecurity-trends-of-2023/]

5. Top 10 cybersecurity Trends for 2023: From Zero Trust to Cyber Insurance [Link: https://thehackernews.com/2023/04/top-10-cybersecurity-trends-for-2023.html?m=1]