Major Security Risks and Mitigation Strategies for 2019

Rafeeq U. Rehman
Email: rafeeq.rehman@gmail.com

July 2019

Executive Summary

CISOs are struggling with prioritizing an ever-increasing scope of work and competing priorities to keep their organizations safe. Many security vendors have published their threat reports, making recommendations to security leaders for better protection of data and networks. This paper short lists major risks identified by these reports and strategies to mitigate these.

There is a very large number of responsibilities for security teams as described in the CISO MindMap. With limited resources on their disposal, CISOs always have to make hard choices prioritizing tasks and project based upon risk assessment. Following are important risks identified by research teams associated with different vendors and corresponding mitigation strategies.

1 Ransomware

RISK – Ransomware is a form of malware that disables computer systems and renders them useless by encrypting data. The attackers typically exploit an existing vulnerability, encrypt data on computers, and demand ransom money to provide keys to decrypt data. Many organizations in diverse industry sectors have fallen victim to these attacks and find them making hard choices of paying the ransom amount or lose their data forever.

Mitigation Strategy

While there is no silver bullet that can guarantee protection against malware/ransomware attacks, following are key items that will help mitigate risk and recover from these attacks.

- Verifiable backup and mock exercise for timely restoration of systems
- Timely patching for vulnerabilities to avoid infection by Ransomware
- Monitoring network traffic for command and control centers activity and timely response to attacks
- Network segmentation to stop lateral propagation of malware if an attack is successful
- Web and email content filtering coupled with awareness programs

2 Phishing Attacks

RISK – Verizon Data Breach Investigations Report (DBIR) shows that phishing emails remain one of the major point of entry for Cyberattacks. Employees fall victim to these mails and click on embedded URLs causing installation of a malware, creation of backdoors, or exfiltration of confidential information to attackers.

Mitigation Strategy

Phishing attacks are difficult to deal with as the attackers get more creative in bypassing email content filtering solutions and trick people into clicking on a URL or takes action with clever emails.

- Robust awareness program
- Web and Email content filtering
- Include executive leadership in tabletop exercises (executives are being targeted more, per DBIR)
- Keep endpoints updated and patched with latest software updates from their respective vendors.

3 Espionage

RISK – Verizon DBIR and other industry reports show that Espionage is a real threat and accounts for

23% of data breaches, overall. While some industry sectors and public organizations with intellectual property are larger targets for espionage activity compared to others, all security leaders should be vigilent and put controls in place to mitigate this risk.

Mitigation Strategy

- Understanding and document your risk profile and potential attackers
- Build threat hunting and dark web investigations practice
- Active monitoring of threats on networks and network segmentation
- Effective awareness program
- Implement a threat intelligence platform to augment SIEM and SOC operations

4 Move to Cloud

RISK – Most organizations are moving to Cloud or have an active Cloud strategy. However, many organization have low skills to fully understand implications and implement controls for Cloud infrastructures (both at network and app levels) resulting in data breaches due to errors and misconfiguration of Cloud environments.

Mitigation Strategy

- Better integration of network with Cloud virtual environment
- Monitoring Cloud environment for potential misconfiguration issues
- Implement Cloud security strategy and controls such as Cloud Access Security Broker (CASB)

5 Emerging Technologies

Risk – Emerging technologies such as Machine Learning (ML), Blockchain, IoT, and autonomous systems are bringing new opportunities and at the same time creating additional attack surface. While many organizations have started utilizing these technologies, security teams are not fully prepared to understand or deal with risks associated with these technologies.

Mitigation Strategy

Following are some key recommendations to manage emerging technologies risk.

- Create internal expertise and a learning culture for these new technologies
- Proactively create policies and procedures for security of emerging technologies
- Engage with internal teams who are planning for using these technologies for better collaborative strategies

Author's Bio

Rafeeq is an author, consultant and an active member of the information risk management community. Based in Columbus OH, Rafeeq works with Verizon global security services group. Rafeeq is author of many books including Linux, Networking and Information Security. Rafeeq has been in leading positions with multiple successful startups, building business using Linux and other open source software technologies. IN addition to his professional work, he is serving as director on boards of multiple non-profit organizations.

Rafeeq holds bachelors and masters degrees in Electrical and Computer Engineering and MBA in Marketing. He also holds industry certifications such as CISSP, CISA, and CISM.

He can be reached via email rafeeq.rehman@gmail.com or at Twitter @rafeeq_rehman.