Cyber Security
Assignment - 2

Dr. G.V. Bansal

Q. 1 Prepare a case study on the Shortage of cyber security Professionals in India, its impact on Organisations and the measures needed to address this challenge. (Discuss the specific implications for the Indian context).

Ans. India's rapid digital transformation has resulted in a severe shortage of cyber security professionals. This case study explores the repercussions on organisations and suggests measures to address this challenge, considering the unique Indian context.

Background of Indian digitalization surge, fueled by factors like cloud adoption and a cashless economy, has heightened cyber threats. The scarcity of cybersecurity experts, estimated at over 1 million poses a critical challenge.

Impact on Organisations:

Increased vulnerability.

Financial consequences.

Stalled Innovation.

Implications for the Indian context:

→ Small and medium sized enterprises are particularly at risk due to limited resources and expertise.

→ Sectors like healthcare and finance face elevated risks, impacting public safety and national security.

measures to address the challenges:

→ Collaborative efforts b/w educational institutions industry bodies and government agencies to develop robust cybersecurity education programs.

→ Initiatives to raise awareness about cyber security careers and emphasize its importance in the digital era.

→ Facilitating collaborations to exchange knowledge, resources, and best practices strengthening cyber security ecosystem.

Conclusion:- Bridging the cybersecurity talent gap in India requires concerted efforts from government, industry and academia. By investing in education, awareness and strategic partnerships, India can fortify its digital landscape ensuring a secure future for organizations and citizens.

Q.2 Analyze a significant cyber attack(s) that has affected an Indian organization or institution. Evaluate the specific challenges faced the response to the incident and the lessons learned.

Ans In August 2018, Cosmos Bank one of the oldest banks in India fell victim to a cyber attack. The attackers used malware infected servers to compromise the bank's system, conducting unauthorized transactions and siphoning funds.

The attackers used sophisticated techniques including leveraging malware and executing a series of fraudulent transactions.

The speed with which the attack was executed posed a challenge in detecting and responding to the incident promptly.

Response to the incident:-

① Isolation and investigation
② Co-ordination with authorities
③ Lessons learned:-

① Enhanced security measures
② Employee training
③ Collaboration and information sharing
④ It is crucial that the landscape of cyber threats is dynamic, and new incidents may have occurred since my last update. Stay informed through reliable news sources and official statements for the latest information on cyber attacks affecting Indian orgs.

Q.3 Investigate the top cybersecurity problems faced by universities and colleges with a focus on the specific types of cyberattacks targeting higher education institutions.

Ans. Top cyber security problems in higher education:-

① Phishing attacks:-
Problem:- Deceptive emails targeting students and staff.
Impact:- Compromised credentials and potential data breaches.

② Ransomware attacks:-
Problem:- Encryption of critical data for ransom.
Impact:- Disruption of activities and financial losses.

③ Data Breaches:-
Unauthorized access to sensitive data.
Compromised personal information and reputational damage.

④ Inside threats:-
Malicious or unintentional actions from students, faculty or staff.

Impact:- Compromised data integrity and unauthorized access.

⑤ DDOS attacks:-

Problem:- overwhelming network and online platforms.

Impact:- Service unavailability and disruption of online learning.

⑥ Inadequate cybe security awareness.

⑦ Vulnerabilities in IT infrastructure.

⑧ Supply chain attacks.

TO address these challenges, universities need comprehensive cybersecurity measures, including training access controls, network monitoring and advanced threat detection technologies. cultivating cybersecurity aware culture is crucial for effective risk mitigation.

Q.4 Select and analyse three real-world malware attacks, covering different malware types such as viruses, worms and ransomware. For each case, describe the attack vector the target the impact.

Ans. 1. Stuxnet (worm):-

Attack vector:- Exploited zero-day vulnerabilities in Windows systems spreading through removable drives and network shares.

Target:- Iran's nuclear facilities, specifically SCADA systems controlling uranium enrichment.

Impact:- Physically damaged centrifuges, significantly impacting Iran's nuclear program.

② WannaCry (Ransomware):-

Attack vector:- Used the EternalBlue exploit, targeting a Windows SMB vulnerability and spread like a worm within networks.

Target:- Global organizations across various sectors including healthcare and finance.

Impact:- Encrypted files, demanded ransom in Bitcoin causing widespread disruption and financial losses.

③ Mydoom (virus):-

Attack vector:- Spread via email attachments or links disguised as delivery failure notifications or other seemingly legitimate communications.

Target:- Microsoft Windows systems creating a botnet for remote control.

Impact:- Rapidly spread causing network congestion disrupting email services and enabling DDoS attacks against specific websites.

Q.5 Provide comparative analysis on DES, AES, RSA.

Ans:- DES:- Data Encryption Standard

AES:- Advanced Encryption Standard

RSA:- Rivest - Shamir - Adleman:-

Comparative Analysis:-

① Key management:-

DES:- Requires secure key distribution due to its symmetric nature.

AES:- Symmetric hence more straightforward key management compared to RSA.

RSA:- Asymmetric necessitating careful key distribution but excelling in secure key exchange.

(2) Key length and security:-

DES:- Short key length compromises security.

AES:- offers strong security with various key length options.

RSA:- Security is related to the difficulty of factoring large numbers longer key lengths enhances security.

(3) Computational efficiency:-

DES:- Faster due to simple operations but considered outdated.

AES:- Efficient and widely adopted for its balance between security and performance.

RSA:- More computationally intensive especially with longer key lengths.

(4) Applications:-

DES:- Largely replaced in modern applications due to security concerns.

AES:- Widely used for securing data in various applications.

RSA:- Essential for secure key exchange, digital signatures and asymmetric cryptography applications.