DFA – Module 1 : part 5
Cyber Crime, Incidence Response system
11.02.22

Arijit Chakraborty

11, 2022

The Digital age – cases of data breach

- **1.** Tik Tok sued in UK & EU for billions over use of **kids' PRIVATE data** to benefit unknown 3rd parties (April 2021)- violation of EU & UK Data Protection Laws
- **GDPR & PDP Bill (India)**
- **2. Fake id in Facebook / twitter**
- Asking for money in COVID pandemic
- Posting obscene messages ,
- Political views & personal attacks
- Cyber stalking by fake id s
- Common in case of celebs & social influencers
- **Forensic Auditors investigating with Cyber Police**

Facebook hacking

- **Spyic =** hack into Facebook accounts on target Android devices in 2 ways:
- **Hack Facebook with Keylogger utility**
- Spyic has inbuilt keylogger function.
- Records all keystrokes typed on target device. Next time Victim logs in FB account with password, hacker gets info

Incident Response & Prevention measures
Recommended cyber safety tips

- Use antivirus softwares
- change passwords frequently
- insert firewalls
- Adopt regular scanning against spyware
- install software patches
- uninstall unnecessary software
- separate user accounts
- maintain backup
- check security settings
- Perform IT audits

Zero Trust principle- Security Framework : 2021

- **“trust but verify” - Traditional security framework**
- Requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

Case Study
GST Network's IT & Cybersecurity Controls

- ***GST Network (GSTN) :*** *well crafted IT and security mechanism based on an advance security architecture*
- ***built around threats and risk mitigating principles***
- ***covering both physical & software security***

GSTN – Platform Approach

- **Platform approach**, enabled to integrate
- banks,
- RBI,
- GST Suvidha Providers
- other functional & technical stakeholders.

❑ **Agile methodology** software development (DevOps)

❑ RBAC = role-based data access system

GSTN – Cyber-Threat Mitigation

- GSTN followed & embedded major threats mitigating principles
- **Cybercrime Risks considered :**

1. data tampering attempts for commercial benefit by individuals or groups,
2. industrial espionage,
3. insider and external attacks to steal or tamper data,
4. cyber attacks on GST system and
5. unauthorized data and system access.

CISO Comments on cyber attack @ GSTN

- *“GSTN network is under continuous cyberattack but we have our own security operations command and control centre.*
- *We have optimised our monitoring framework in such a way that none of the attacks was able to surpass even the first layer of security so far.*
- *You cannot stop the security attacks but you can mix the security control at your end in such a way that it should not pass the security gates,“*
- *---- - Anand Pande, Senior Vice President – CISO, GSTN.*

RFT

FOR

ANNUAL CYBERSECURITY & SYSTEMS AUDIT

Ref: ECGC/Tender-06/RMD/11/2021-22

Date: 21-01-2022

ECGC LIMITED

10th Floor, Express Tower, Nariman Point, Mumbai - 400021

Cyber Security Audit- ECGC

- **Purpose of Cyber security Audit**
- ECGC envisages review of processes & IT infrastructure with respect to :
- 1. Review based on IRDAI Circular Ref No: IRDA/IT/GDL/MISC/082/04/2017 dated 07.04.2017 (Guidelines on Information and Cyber Security for Insurers) amended vide its Ref. No: IRDA/IT/CIR/MISC/ 301/12/2020 dated 29/12/2020
- 2. ITGC (General Controls) Audit for IT systems handling Financial Information
- 3. Vulnerability Assessment and Penetration Testing of IT Systems
- The auditor shall also assist ECGC Ltd. in the following areas pertaining to IRDAI Circulars -
- 1. Adhering to changed or updated timelines of compliance
- 2. Adhering to further clarifications issued by IRDAI
- 3. Providing additional certification/s and clarifications as required by the IRDAI from the cyber security auditor

Cyber Audit Scope

- Testing of Applications,
- Review of Information Security Policy & Procedures,
- Gap Assessment in IT security and Procedures,
- Assessment of Network Security & Information Security solutions,
- Vulnerability and Penetration testing,
- Review of Data Centre including physical visits, compliance with IRDAI, and submission of reports.
- Backbone IT infrastructure located at Mumbai
- Data Centre at Faridabad

Exam related MCQ

- **1. MCAfee is an example of**
- A. Photo Editing Software
- B. Quick Heal
- C. Virus
- D. Antivirus
- **2. Which of the following is known as Malicious software?**
- A. illegalware
- B. badware
- C. malware
- D. maliciousware

- **3. To protect a computer from virus, user should install -------- in his computer.**
- A. backup wizard
- B. disk cleanup
- C. antivirus
- D. disk defragmenter
- **4. VIRUS stands for**
- A. Very Intelligent Result Until Source
- B. Very Interchanged Resource Under Search
- C. Vital Information Resource Under Siege
- D. Viral Important Record User Searched

- **5. Which of the following is/are threats for electronic payment systems?**
- A. Computer worms
- B. Computer virus
- C. Trojan horse
- D. All of the above
- **6. Key logger is a**
- A. Firmware
- B. Antivirus
- C. Spyware
- D. All of the above

- **7. A -------- is a computer program that can replicate itself and spread from one computer to another.**
- A. Antivurs
- B. PenDrive
- C. Mouse
- D. Computer Virus
- **8. Authentication is**
- A. modification
- B. insertion
- C. assure identity of user on a remote system
- D. none of the above

- **9. A ------- is a computer program that can invade Laptop & perform variety of functions from annoying(e.g. popping up messages) to dangerous (e.g. deleting files or destroying hard disk).**
- A. Ms Word
- B. Ms Access
- C. Antivirus
- D. Computer Virus
- **10. Which are the reasons for committing cyber crime :**
- A. Identity of attacker is unknown
- B. attack may be done remotely
- C. Fraud may not be discovered quickly
- D. It is considered ‘’ work of art’’ by some hackers
- Options
- 1. A & B
- 2. B&C
- 3. A,B,C
- 4. A,B,C,D