Digital India Power To Empower | Azadi Ka Amrit Mahotsav | certin

MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY GOVERNMENT OF INDIA
सत्यमेव जयते

OPEN, SAFE & TRUSTED AND ACCOUNTABLE INTERNET

FREQUENTLY ASKED QUESTIONS (FAQs) On Cyber Security Directions of 28.04.2022

(under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents)

Table of Contents

Introduction

India is fast becoming one of the world's largest connected nations - with over 80 Crores Indians presently connected and using the Internet and cyberspace - and with this number expected to touch 120 Crores in coming few years. The Internet also represents an important part of our Economy - with the vibrant Startup Eco-system, Global investors and an objective of $1Trillion Digital Economy by 2026. While the Internet represents opportunity and innovation, it also represents online safety challenges, user harm and cybercrimes. So, to both achieve our goals as well as to deal with the challenges, our policy objectives are led by Laws and Rules that will ensure that the Internet and Cyberspace are Open, Safe & Trusted and Accountable.

2. CERT-In is an organization that is tasked with ensuring safety of the Internet in India. The Government of India appointed "Indian Computer Emergency Response Team (CERT-In)" vide notification dated 27th October 2009 published in the official Gazette in terms of the provisions of sub-section (1) of section 70B of the Information Technology Act, 2000 (IT Act, 2000). As per provisions of sub-section (4) of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security:-

a) collection, analysis and dissemination of information on cyber incidents;
b) forecast and alerts of cyber security incidents;
c) emergency measures for handling cyber security incidents;
d) coordination of cyber incident response activities;
e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f) such other functions relating to cyber security as may be prescribed.

3. The provisions of sub-section (5) of section 70B of the Information Technology Act, 2000 provides that "The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed." In this regard, Central Government in exercise of powers conferred by clause (zf) of section 87 read with sub-section (5) of section 70B of the Information Technology Act, 2000 has notified the "Information Technology (The Indian Computer Emergency Response Team and

Manner of Performing Functions and Duties) Rules, 2013" published vide notification dated 16th January 2014. These rules regulate the manner of performing functions and duties by the Indian Computer Emergency Response Team.

4. In accordance with the provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person for carrying out the provisions enshrined in sub-section (4) of section 70B of the IT Act, 2000. Further, the provisions of sub section (7) of section 70B of the IT Act, 2000 enunciates that *"Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both."*

5. Stakeholder consultations were held on the Draft Cyber Security Directions in March 2022, before they were finalized.

6. The following FAQs have been prepared to explain the nuances of Cyber Security Directions of 28.04.2022 issued under sub-section (6) of section 70B of the Information Technology Act, 2000 administered by MeitY for enabling better understanding of the various stakeholders in order to seek compliance to promote Open, Safe & Trusted and Accountable Internet in the country.

Note: This document is in response to general queries received by CERT-In from time to time. It is not a legal document and in no way whatsoever replaces, amends or alters any part of the IT Act, 2000 and/or the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (hereinafter referred as CERT-In Rules, 2013). The FAQ is an evolving document and hence, the version of this document may undergo changes.

Section I:
Basic Terminology and Scope of the Directions

Q 1. What is the reason for these Cyber Security Directions?

Ans: The Internet in India is growing fast and over the next few years over 120 Crore Indians will have access to the Internet and use it for business, education, finance and myriad other applications and services including Digital Government services. The Internet has seen growth in innovation and at the same time it has seen rise in crimes, user harm and other challenges to online safety. It is the Government of India's policy goal to ensure that Indian Internet users experience a Safe & Trusted Internet. Cyber Security Directions are a part of the overall framework of ensuring online safety and trust for users.

Q 2. What is CERT-In and what is the status of CERT-In?

Ans.: 'Indian Computer Emergency Response Team' (CERT-In) is the national agency for cyber security incident response and proactive measures for prevention of cyber incidents in the Country. CERT-In has been appointed by Central Government vide notification dated 27th October 2009 in terms of the provisions of section 70B (1) of The Information Technology Act, 2000 (IT Act, 2000).

Q 3. What is Cyber Security Incident?

Ans.: "Cyber Security Incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes in data, information without authorisation.

Q 4. Why Cyber Security is important?

Ans.: The digital technology and usage of internet has grown exponentially and is integral part of modern life. Today, cyberspace is the common platform used by citizens, businesses and Governments for communication, dissemination of information, e-commerce, services, economic activities, education, entertainment etc. At the same time, the advancement of technology has opened vulnerabilities for exploitation by the

malicious actors. Cyber security is the protection of electronic data and information. To deal with the emerging cyber threat landscape and to ensure safe usage of digital technologies by users, the legal, technical, organizational and collaborative measures need to be taken by stakeholders.

Q 5. What process was followed to arrive at the Cyber Security Directions of 28.04.2022?

Ans.: CERT-In is in operation since the year 2004. Based on analysis of cyber security incidents and trends certain gaps in processes of organisations and service providers have been observed by CERT-In. Accordingly, consultations with the industry and Government organisations have been held from time to time and based upon the inputs received from the stakeholders, draft directions were framed. Subsequently, CERT-In under the aegis of MeitY held stakeholder consultation in March 2022 towards finalisation of the directions.

Q 6. What are the functions of CERT-In in the area of cyber security?

Ans.: CERT-In performs the statutory functions in the area of Cyber Security as specified in sub-section (4) of section 70B of the Information Technology Act, 2000, which enshrines that CERT-In shall serve as the national agency for performing the following functions in the area of cyber security :-

a) collection, analysis and dissemination of information on cyber incidents;
b) forecast and alerts of cyber security incidents;
c) emergency measures for handling cyber security incidents;
d) coordination of cyber incident response activities;
e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f) such other functions relating to cyber security as may be prescribed.

Q 7. Who do these Cyber Security Directions of 28.04.2022 apply to?

Ans.: Service providers, intermediaries, data centres, body corporate, Virtual Private Server (VPS) providers, Cloud service providers , VPN Service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and Government organisations shall follow these Cyber Security Directions of 28.4.2022 as applicable to them. Individual citizens are not covered by these Directions.

Q 8. What is the applicability of provisions of the Information Technology Act, 2000 vis. a vis. other provisions of any other law in the matter of cyber security?

Ans.: Section 81 of the Information Technology Act, 2000, which is reproduced below may be referred:

"The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force."

Q 9. The type of incidents mentioned in the Cyber Security Directions of 28.04.2022 brought out in the annexure may be clarified. Some of them are very broad such as "attacks on applications such as e-governance, e-commerce, etc.; compromise of critical systems/information". Some guidance with respect to the interpretation of the terms used will be helpful.

Ans.: An illustrative list of explanation of the types of incidents required to be reported to CERT-In are given in this FAQ at Annexure I.

Q 10. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provide that *"The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team".* Do intermediaries have to mandatorily report any and all cyber security incidents or only those specified in the Annexure to the Rules?

Ans.: It is correct that the intermediaries as defined under the Information Technology Act and Rules made thereunder to report cyber security incidents and share any related information thereof with CERT-In. The Rule 3(1) (l) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provides that *"The intermediary shall report cyber security incidents and share related information with the Indian Computer Emergency Response Team in accordance with the policies and procedures as mentioned in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013".* In this context, it is obligatory to note that in terms of Rule 12 of the CERT-In Rules 2013, the type of cyber security incidents as identified in the Annexure [of the Rules] and also brought out in the Cyber Security Directions of 28.04.2022, are to be mandatorily reported to CERT-In by any organization or corporate entity, including intermediaries affected by cyber security incidents as early as possible to leave scope for action.

It is, thus, imperative that the intermediaries also report those types of cyber security incidents which are not mentioned either in the annexure of the CERT-In Rules, 2013 or in the Cyber Security Directions of 28.04.2022, to CERT-In considering the nature, severity and impact of the incident.

Q 11. What is the difference between the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and Cyber Security Directions of 28.04.2022 in terms of applicability thereof?

Ans.: The provisions of Part-II of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 is applicable to Intermediaries read with relevant provisions of Part-I whereas Cyber Security Directions of 28.4.2022 are not limited to Intermediaries but are applicable to service providers, intermediaries, data centres, body corporate, Virtual Private Server (VPS) providers, Cloud service providers, VPN Service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and Government organisations.

Q 12. What is the method of reporting and format for incident reporting? Will it be updated?

Ans.: The details regarding methods and formats of reporting cyber security incidents is published on the CERT-In website https://www.cert-in.org.in and will be updated from time to time.

Q 13. Where multiple parties are 'affected' by a cyber security incident, for example - consumer-facing business and its back-end / outsourcing partner, who needs to report when the attack has occurred on the servers of outsourcing partner but data of consumer facing business is compromised ? Can it be a joint reporting to CERT-In? Can it be contractually agreed on who bears the reporting obligation?

Ans.: Any entity which notices the cyber security incident, shall report to CERT-In. The obligation of reporting of cyber incident is neither transferrable nor indemnified or dispense with.

Q 14. What is the usual process followed by CERT-In after the incident reporting?

Ans.: CERT-In, after receiving the information about the cyber security incident reported to it, conducts analysis of the same and coordinates with relevant entities

including providing assistance to the affected entities to deal with incident. CERT-In in discharge of its mandate may call for information and give directions to the entities in terms of sub-section (6) of section 70B of the IT Act, 2000. CERT-In may issue advisories, guidelines, vulnerability notes, white papers etc. as deemed appropriate.

Q 15. Rule 12 (1) (a) 2nd para, refers to vulnerability reporting. Please clarify that this is not a mandatory but a voluntary process.

Ans.: Rule 12(1) (a) of the CERT-In Rules, 2013 is about reporting of Cyber security incidents whereas its second paragraph provides details regarding methods and formats for reporting cyber security incidents, vulnerability reporting and remediation, incident response procedures and dissemination of information on cyber security. The terms "Cyber security incident" and "Vulnerability" are defined in rule 2(h) and rule 2(p) of the CERT-In Rules, 2013, respectively. At present, the reporting of vulnerability as a standalone or in isolation, unconnected with the cyber security incident is not mandatory.

Q 16. What is the policy for disclosure of information relating to cyber security incidents reported to CERT-In?

Ans.: The disclosure of information by CERT-In is governed by provisions of Rule 13 of CERT-In Rules, 2013 subject to applicable law.

Q 17. What process does CERT-In follow to ensure chain-of-custody of information provided?

Ans.: CERT-In functions in accordance with the provisions of CERT-In Rules, 2013 as prescribed in terms of provisions of section 70B (5) of the IT Act, 2000. Hence, the provisions of CERT-In Rules, 2013 may be referred to.

Section II:
Directions under sub-section (6) of section 70B of the IT Act, 2000

Q 18. What areas do the Cyber Security Directions of 28.04.2022 cover?

Ans.: These directions have been issued to augment and strengthen online safety and cyber security, in turn to ensure Safe & Trusted and Accountable Internet in the country. These directions issued to service providers, intermediaries, data centres, body corporate and government organisations cover synchronization of ICT system clocks, reporting of cyber incidents to CERT-In, types of cyber incidents to be reported, maintaining logs of ICT systems, registration of information about subscribers/customers and maintaining KYC records by Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers, Virtual Private Network Service (VPN Service) providers, virtual asset service providers, virtual asset exchange providers and custodian wallet providers.

Q 19. How do the Cyber Security Directions of 28.04.2022 ensure Open, Safe & Trusted and Accountable Internet for citizens?

Ans.: These directions are intended to ensure timely reporting of cyber incidents to CERT-In, supplemented by necessary information required for analysis of such incidents which will enhance cyber security situational awareness, mitigation of cyber security incidents/attacks and coordinated incident response measures thereby ensuring protection of data/information and availability of services to citizens. These efforts will enhance overall cyber security posture and ensure Open, Safe & Trusted and Accountable Internet in the country.

Q 20. Do the Cyber Security Directions of 28.04.2022 affect the Right to Privacy of individuals?

Ans.: The right to informational privacy of individuals is not affected by these Cyber Security Directions of 28.04.2022. These directions do not envisage seeking of information by CERT-In from the service providers on continuation basis as a standing arrangement. CERT-In may seek information from service providers in case of cyber security incidents and cyber incidents, on case to case basis, for discharge of its statutory obligations to enhance cyber security in the country. The service providers are bound to protect the users' information by following reasonable security practises and procedures.

Q 21. How do the Cyber Security Directions of 28.04.2022 benefit users in the country?

Ans.: In the era of substantial digitization of the way of life, cyber security is crucial to prevent stealing of identity, financial information and other sensitive information of users by malicious actors. Cyber security is an essential aspect for public good. These Cyber Security Directions of 28.04.2022 are intended to mandate cyber security best practices by the service providers and organisations so that safety of users' data is ensured and trusted services are available to users on continuous basis. The cyber incident can affect one or many entities, therefore, it is imperative that all incidents are tracked and investigated to deduce inter-linkages between them in order to provide Safe & Trusted Internet usage to citizens. Implementation of the measures mandated in these directions will facilitate timely detection & mitigation of breaches and effective investigation of cyber crimes.

Q 22. Do I need to report incidents to CERT-In even if I have contractual obligation of not to disclose any details with my customer?

Ans.: The obligation of reporting of Cyber Security incidents to CERT-In as enshrined in Section 70B of the IT Act, 2000 read with CERT-In Rules, 2013 is statutory in nature and overrides any confidentiality clause in any contract by virtue of the provisions of section 81 of the IT Act, 2000.

Q 23. What would be the implications or impact of non-compliance? Are there any penalties that body corporate, service providers, intermediaries, data centres may face under these Cyber Security Directions of 28.04.2022?

Ans.: The act of non-compliance of Cyber Security Directions of 28.04.2022 issued under sub-section (6) of section 70B of the Information Technology Act, 2000 may attract the penal provisions of sub-section (7) of section 70B of the Act. This power will be exercised reasonably and on occasions when the non-compliance is deliberate.

Q 24. What are the implications if an incident remains undetected for a long duration? What time frame for reporting will be applicable and from when?

Ans.: Organisations need to deploy appropriate security controls and follow reasonable security practices to detect and prevent cyber security incidents. The cyber incident needs to be reported to CERT-In within 6 hours of noticing the incident or being brought to notice about such incident. Based on analysis of reported incidents, the gaps in

security processes can be analysed to enhance ability of the organisations to detect and mitigate the incidents in a timely manner.

Q 25. What is the scope of "body corporate"? Does it include any and all types of entities irrespective of their business?

Ans.: The term "body corporate" has been explained under section 43A of the Information Technology Act, 2000, which is reproduced below:

"body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

Q 26. Do the Cyber Security Directions of 28.04.2022 apply only to Indian companies or also to foreign firms that serve Indian customers?

Ans.: The provisions of the Information Technology Act, 2000, in particular the provisions of section 1 and section 75 of the Act may be referred to. These Cyber Security Directions of 28.04.2022 are applicable to any entity whatsoever, in the matter of cyber incidents and cyber security incidents.

Q 27. Whether the Cyber Security Directions of 28.04.2022 are applicable to virtual asset service providers, virtual asset exchange providers and custodian wallet providers not located in India but catering to Indian users?

Ans.: These Cyber Security Directions of 28.04.2022 are applicable to any entity only in the matter of cyber incidents and cyber security incidents.

Q 28. Whether the Cyber Security Directions of 28.04.2022 are applicable to online gaming companies?

Ans.: These Cyber Security Directions of 28.04.2022 are applicable to all entities in so far as reporting of a cyber incident is concerned.

Q 29. Are those service providers who do not have a physical presence in India required to designate a Point of Contact?

Ans.: The service providers, intermediaries, data centres and body corporate offering services to the users in the country shall designate a Point of Contact to liaise with CERT-In.

Q 30. The Cyber Security Directions of 28.04.2022 require reporting cyber incidents within 6 hours. What if all the information as per the CERT-In incident reporting form (https://www.cert-in.org.in/PDF/certinirform.pdf) is not available within such time?

Ans.: The entities may provide information to the extent available at the time of reporting. Additional information may be reported later within reasonable time to CERT-In.

Any incident as stated in Annexure-I of the Cyber Security Directions of 28.04.2022 and meeting the following criteria should be reported within the stipulated 6 hour time:

- cyber incidents and cyber security incidents of severe nature (such as denial of service, distributed denial of service, intrusion, spread of computer contaminant including Ransomware) on any part of the public information infrastructure including backbone network infrastructure
- Data Breaches or Data Leaks
- large-scale or most frequent incidents such as intrusion into computer resource, websites etc.
- cyber incidents impacting safety of human beings

Q 31. Are entities required to report information regarding cyber security incidents which has affected their data stored in a third party's systems?

Ans.: The Cyber Security Directions of 28.04.2022 are applicable to all entities in so far as reporting of a cyber incident is concerned.

Q 32. How is the confidentiality of the customer data collected by the service providers ensured? What should an organization do in case logs contain PII of data subjects of a foreign data protection regime such as GDPR with extra-territorial application?

Ans.: The requirements on the part of service providers, intermediaries and body corporate in respect of protection of confidentiality of the customer data prior to the issuance of these Cyber Security Directions of 28.04.2022 are in force and does not change.

Q 33. With reference to the requirements of registering information by Data Centres, VPS providers, Cloud Service providers and VPN Service providers, what

is meant by "Ownership pattern of the subscribers / customers hiring services"?

Ans.: The Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and VPN Service providers are required to maintain basic information about customers/subscribers who use their services viz. individual, partnership, association, company etc. of whatsoever nature, with brief particulars of key management. The maintenance of such data in safe & secure manner as is expected for all entities operating in India.

Q. 34. The Cyber Security Directions of 28.04.2022 require Virtual Private Network Service (VPN Service) providers to register and maintain certain specific information about the subscribers/customers. Does this direction apply to Enterprise/Corporate VPNs as well?

Ans.: No. For the purpose of this direction, VPN Service provider refer to an entity that provide "Internet proxy like services" through the use of VPN technologies, standard or proprietary, to general Internet subscribers/users.

Q 35. Is it required to store copy of logs in India only?

Ans.: The logs may be stored outside India also as long as the obligation to produce logs to CERT-In is adhered to by the entities in a reasonable time.

Q 36. Do we need to store logs of Foreign Service providers and foreign part of financial transactions in India?

Ans.: Any service provider offering services to the users in the country needs to enable and maintain logs and records of financial transactions in Indian jurisdiction.

Q 37. What logs need to be stored for ICT systems to help in cyber incident analysis?

Ans.: The logs that should be maintained depend on the sector that the organisation is in, such as Firewall logs, Intrusion Prevention Systems logs, SIEM logs, web / database/ mail / FTP / Proxy server logs, Event logs of critical systems, Application logs, ATM switch logs, SSH logs, VPN logs etc. It may be noted that this list of logs is not exhaustive but has been mentioned to provide flavour of logs to be maintained by the relevant teams. From the incident response and analysis perspective both successful as well as unsuccessful events shall be recorded.

Q 38. Which authority can request logs from entities?

Ans.: The requisition for seeking information is respect of logs may be given by an officer of CERT-In not below the rank of Deputy Secretary to the Government of India for carrying out the functions provided in sub-section(4) of section 70B of the IT Act, 2000.

Q 39. Why is it required to synchronize ICT systems clocks?

Ans.: A typical cyber incident involves multiple computer systems within as well as across entities. Without an accurate time stamp it is extremely challenging to re-create accurate sequence of events thus causing serious hindrance while handling cyber incidents. Moreover, security technologies also rely heavily on specific patterns and correlation rules that are often based on time parameter, therefore, unsynchronised clocks across systems could result in failure of security systems as well as entity's ability to act on proactive alerting/advisory of CERT-In as well as other agencies.

Q 40. Is it required to synchronise clocks only with NTP Servers of NPL and NIC? Is it now required to set system clocks in Indian Standard Time (IST) only?

Ans.: The requirement of synchronising time is stipulated to ensure that only standard time facilities are used across all entities. Organisations may use accurate and standard time source other than National Physical Laboratory (NPL) and National Informatics Centre (NIC) as long as the accuracy of time is maintained by ensuring that the time source used conforms to time provided by NTP Servers of NPL and NIC.

Also, there is no need to mandatorily set system clocks in Indian Standard Time (IST). NTP Server provides time stamp in UTC, the conversion of UTC to local time is done at the host which receives the NTP sync from the NTP Server. NPL or NIC also provides UTC time as per global norms. The current directive requires uniform time synchronisation across all ICT systems irrespective of time zone. The time zone information shall also be recorded along-with time to facilitate accurate conversion at the time of need.

Q 41. Organisations having ICT infrastructures spanning multiple geographies, such as Cloud Service Providers, use internally setup global NTP servers which are typically synchronized with external time sources. Synchronizing the clocks

differently in ICT portion located in India could pose technical issues. Can they continue with their original method of time synchronisation for ICT Infrastructure in India?

Ans.: The need for synchronising time is stipulated to ensure that only standard time facilities are used across all entities. Organisations having ICT infrastructures spanning multiple geographies may use accurate and standard time source other than National Physical Laboratory (NPL) and National Informatics Centre (NIC), however, it is to be ensured that their time source shall not deviate from NPL and NIC.

Q 42. ICT infrastructure that runs on Cloud uses time sources inherent within the Cloud. Is it now required to discontinue with the current practice and sync only with the NIC and NPL?

Ans.: Cloud ICT Infrastructures that span multiple geographies typically setup their own NTP servers to ensure conformity of time across entire ICT infrastructure as well as to enable them to handle complexities arising out of situations like leap smearing in a uniform way. As per the directive, a common standard time source is required and it also permits the use of accurate and standard time source other than NPL and NIC for large ICT infrastructure, however, it is to be ensured that their time source shall not deviate from NPL and NIC.

Customers in cloud environments, on the other hand, have an option to use the native time services offered by the Cloud to synchronize their clock or they can also set up their own NTP server within their cloud environment. The entities relying on the native time services offered as part of Cloud may continue to use the same, however, if any entity operates their own NTP service (using NTP server or any other device), which synchronises with time sources other than native cloud time services, the NTP Servers of NPL, NIC or other accurate and standard time sources may be used as long as the accuracy of time is maintained. It is to be ensured that time source other than NIC/NPL, if used, shall not deviate from NPL and NIC.

Q 43. How to synchronize systems clocks with the NTP Server of National Informatics Centre or National Physical Laboratory?

Ans.: System clocks can be synchronised by configuring NTP Servers of the NIC or NPL as a time source in the enterprise NTP Server (or on the device being used as NTP Server/s for the enterprise).

The details of NTP Servers of NIC and NPL are currently as follows:

National Informatics Centre (NIC) :
samay1.nic.in
samay2.nic.in

National Physical Laboratory :
time.nplindia.org

Q 44. Since when will the Cyber Security Directions of 28.04.2022 will come into effect?

Ans.: These Cyber Security Directions of 28.04.2022 will become effective after 60 days from the date of issuance.

Annexure-I

Explanation for Types of Cyber Security Incidents to be Reported to CERT-In

i. Targeted scanning/probing of critical networks/systems

Targeted network scanning/probing refers to the action of gathering information regarding critical computing systems and networks, thus, impacting the confidentiality of the systems. It is used by adversaries to identify available network hosts, services and applications, presence of security devices as well as known vulnerabilities to plan attack strategies.

ii. Compromise of critical systems/information

Gaining control of computer resource without permission typically through exploitation of a vulnerabilities. Attack methods for compromise may include "shoulder surfing", "social engineering", "exploitation of software vulnerability", "sophisticated malware" etc.

Compromise of critical systems/information may impact all core aspects of cyber security viz. confidentiality, integrity and availability.

iii. Unauthorised access of IT systems/data

Accessing systems / data without authorisation thereby impacting the confidentiality of the system. This incident may involve compromising the systems, poor security controls, weak credentials and /or privilege escalation etc.

iv. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.

Defacement typically refers to website compromise with the intention to alter the appearance of a webpage. Some defacement attacks involve inserting new web-pages as well. Such attack primarily affects the integrity of the website.

A more sinister form of website compromise involves insertion of malicious script/code, links to external websites for the purpose of spreading malware. This attack typically does not result in any visible change on the website appearance, thus, harder to detect and prevent.

v. Malicious code attacks such as spreading of Virus/Worm/Trojan/Bots/ Spyware/Ransomware/Cryptominers

Malicious code or malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malicious code is hostile, intrusive, or annoying software or program code and could impact confidentiality, integrity as well as availability of the system.

Virus: A computer virus replicates itself by modifying other computer programs and inserting its own code. It is not standalone program and attaches to another system processes/program/documents.

Worm: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.

Trojan: Trojan horse is any malware that misleads users of its true intent.

Bots: A bot, short for "robot", is a type of malware that performs automated tasks on commands from malicious actors.

Spyware: Spyware is software with malicious behaviour that aims to gather information about a person or organization and send it to another entity.

Ransomware: a type of malicious software designed to block access to a computer system, commonly by encrypting the files on the system, until a sum of money is paid.

Cryptominers: malicious code designed to hijack idle processing power of a victim's device and use it to mine cryptocurrency.

vi. Attack on servers such as Database, Mail and DNS and network devices such as Routers

DNS Hijacking is modification of DNS records with intention to redirecting the victim to malicious domains/IPs. DNS Cache Poisoning involves corrupting the DNS server's cache with fake values causing the name server to return incorrect result thereby redirecting the victim to malicious domains/IPs. Routers are the traffic controllers of the Internet and ensure flow of information from source to destination. Routing disruption could lead to massive routing errors resulting in disruption of Internet communications.

Compromise of Mail / Database servers impacts all core aspects of cyber security viz. confidentiality, integrity and availability.

vii. Identity Theft, spoofing and phishing attacks

Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud.

Spoofing is a technique used to conduct Identity theft in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Phishing is an attack aimed at stealing sensitive personal data that can lead to committing online frauds. Phishing is also used to gain access to user's credentials for espionage. Such incidents primarily targets confidentiality aspect of the system and/or user.

viii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks

Denial of Service (DoS) attack is an attempt to make a computer resource unavailable to intended users.

Distributed Denial of Service (DDoS) attacks occurs when multiple compromised/misconfigured computer systems flood the communication link (a.k.a. bandwidth) or resources (CPU, memory) of a targeted system.

ix. Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks

SCADA systems are used for monitoring, and remotely controlling, geographically widely distributed processes from a centralised location. They have been incorporated for operational purposes in most of the critical infrastructure.

Sophisticated malware are used by threat actors to target SCADA systems. The effect of these attacks can range from espionage to cause disruption of essential services.

This type of incidents impacts all core aspects of cyber security viz. confidentiality, integrity and availability.

x. Attacks on Application such as E-Governance, E-Commerce etc.

Software code of the Applications is often affected by application vulnerabilities like SQL Injection, Cross Site Scripting (XSS), Cross-Site Request Forgery (CSRF) etc. Attackers leverage these vulnerabilities to target important infrastructure like E-Governance, E-Commerce infrastructure etc. Such cyber-attacks on E-Governance and E-Commerce applications may cause adverse impact on availability of services, impair confidentiality and integrity of data/information.

xi. Data Breach

A Data Breach is a cyber-incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or theft of Intellectual property etc. Most data breaches are caused due to un-plugged vulnerabilities, hacking or malware attacks.

Data Breaches primarily results in loss of confidentiality of the information.

xii. Data Leak

Data Leak is the release of sensitive, confidential or protected data to an untrusted environment. Data Leaks can be used by threat actors for malicious activities and can be due to accidental causes such as lack of proper safeguards to protect data, improper configuration, user error, backdoors, vulnerabilities etc.

Similar to Data Breach, Data Leak also results in loss of confidentiality of the information.

xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers

Attacks targeting IoT devices such as cameras, routers, DVRs and wearables are increasing. The compromise of these devices further acts as an intrusion point for attackers to gain access to internal network of the organisation leading to disruption of services, data theft, possible espionage amongst others. IoT devices have also been targeted for creating botnets such as Mirai etc.

This type of incidents impacts all core aspects of cyber security viz. confidentiality, integrity and availability.

xiv. Attacks or incident affecting Digital Payment systems

The rise of Digital payment landscape is coupled with increasing cyber-incidents and attacks on digital payment infrastructure. Attackers target Digital payment instruments; IT infrastructure of financial institutions, depositors; SWIFT network, ATM switch using a variety of attack techniques such as vulnerability exploitation, sophisticated malwares etc.

This leads to financial and customer data breach, financial frauds, decline in user trust and confidence in digital ecosystem and loss of reputation of the organisation.

Attacks or incident on Digital Payment systems target confidentiality and/or integrity of the systems and data however serious incidents also often results in non-availability of systems.

xv. Attacks through Malicious mobile Apps

With the Smart Phones becoming primary computing devices for consumers as well as their increasing use in the corporate world, smart phones have become lucrative target for compromise through the mobile apps available in the mobile app stores.

Malicious mobile Apps typically target confidentiality of the data stored and processed on the mobile.

xvi. Fake mobile Apps

Fake apps are apps created by cybercriminals to cause harm to users and their devices. They are designed to resemble legitimate apps but instead carry out malicious activities.

Fake Apps fall into two broad categories: Counterfeits (fake apps that imitate a real one) and Repackages (taking an existing app and repackaging it – for example, for showing ads or for inserting malicious code). Both types are also available in the mobile app stores.

Fake mobile Apps primarily target confidentiality of the data stored and processed on the mobile.

xvii. Unauthorised access to social media accounts

Unauthorized access to social media accounts is when a malicious user gains access to someone else's social media account without their consent or knowledge. An attacker may use a variety of techniques to gain credentials of victims' social media account including phishing, Key Loggers, Man-In-The-Middle attack (MITM), Social Engineering, Session Hijacking, Saved Passwords in browser password manager etc.

Unauthorised access to social media accounts of legitimate organisations may result in propagation of fraudulent messages and could impact confidentiality, integrity as well as availability of the affected accounts.

xviii. Attacks or malicious/suspicious activities affecting Cloud computing systems/servers/software/applications

As is the case with conventional computing, cloud is also accompanied by vulnerabilities to targeted attack by malicious actors. The vulnerabilities include Cloud API vulnerabilities, weak cryptography, exposed data repositories and unauthorised access to victims' cloud credentials.

This type of incidents impacts all core aspects of cyber security viz. confidentiality, integrity and availability.

xix. Attacks or malicious/suspicious activities affecting systems/servers/networks/ software/applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones

Development of technology in the field of Big Data, Block chain, virtual asset exchange, custodian wallets etc. have given rise to new cyber security challenges. Emerging technologies are being increasingly adopted by businesses thereby increasing the dependency of business on cyber space and increasing attack surface and evolving threat landscape. Each of the abovementioned areas are highly specialised and have their own risks and threats if reasonable security practices are not followed.

These type of incidents impacts all core aspects of cyber security viz. confidentiality, integrity and availability.

xx. Attacks or malicious/suspicious activities affecting systems/servers/software/ applications related to Artificial Intelligence and Machine Learning

Attacks that target Machine Learning models with the intention to cause a malfunction are a growing threat. The attacks employs various techniques such as deceptive data, environment manipulation etc. to corrupt the model and cause the model to behave erroneously.

This type of incident could have impact on confidentiality, integrity and availability of the affected system.

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India

Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi: 110003