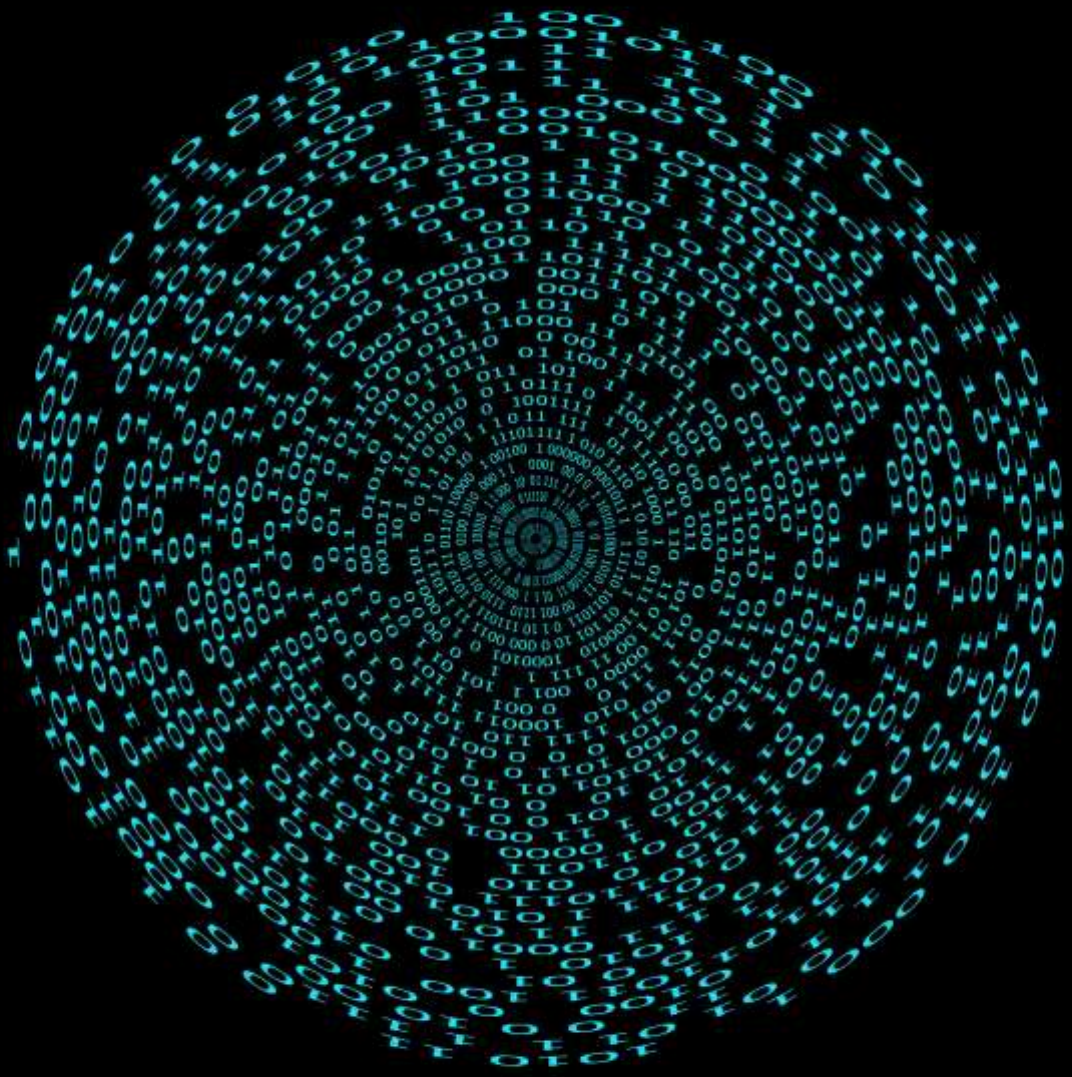
Deloitte.



CyberIntelligenceCenter

CERT-IN's direction for reporting cyber incidents

June 2022

Table of contents

Introduction

On 28 April 2022, the Indian Computer Emergency Response Team (CERT-IN), Issued fresh directions mandating that all cybersecurity incidents (refer to annexure I) compliances in relation to cybersecurity incidents need to be reported to the CERT-IN within six hours from incident identification/notification. Given this stringent timeline, it is imperative for organisations to re-assess their internal cybersecurity controls and capabilities and ensure that robust measures are put in place to meet these directives.

This directive was a welcome move, as prior to this, organisations faced several visibility issues and cybersecurity incidents that remained un-or-under reported. There was broken or no analysis of cybersecurity incidents and missing links in the investigation. This new directive will help organisations strengthen their cybersecurity posture.

Additionally, this directive from CERT-IN will help in improving security posture of national critical infrastructure, prevent reputational losses occurring due to cyberattacks, and prevent any disruptions in the services.

CERT-IN directives

According to the CERT-IN directives, organisations need to adhere to the following:

- Enable logs of all their Information and Communication Technologies (ICT) systems.
- Retain logs for 180 days.
- Report to CERT-IN within six hours of any qualified cybersecurity incidents.
- Report incidents in the specified format (Refer to annexure-II for more details).
- Synchronise time with National Informatics Centre's Network Time Protocol.
- Define a SPOC for this activity and share their credentials with CERT-IN.
- Ensure that Virtual Private Server (VPS) providers, cloud service providers, and Virtual Private Network Service (VPN service) providers maintain accurate information, such as name of the subscriber and IP address for five years. (Refer to annexure-III for more details).

These directives will have implications on organisations, some of which have been outlined below:

- All enterprise assets such as IT, OT, IoT, IIoT come under CERT-IN's purview. Enterprises will need to re-look at the cybersecurity posture at their factories, manufacturing plants, and IT workloads.
- Enterprises should embrace Security Operation Center (SOC) solutions and other applicable from trusted Managed Security Service Providers (MSSPs).
- Enterprises will need to work on the visibility of their critical incidents.
- A structured approach towards all incidents, their remediation, response and reporting to CERT-IN is the need of the hour.
- Implementation of log forwarding to logger/Security Information and Event Management (SIEM) can be an efficient solution.
- Produce logs and incident analysis to CERT-IN when requested.

Key highlights of the CERT-IN directives

The CERT-IN directive is all set to become a law from 27 June 2022. This new direction, released jointly by MeitY and CERT-IN, falls under Sub-section (6) of Section 70B of the Information Technology Act, 2000 and mandates the following:

Applicability
All organisations that come under the purview of the IT Act, 2000 will be a part of this directive. The directive will include all service providers, intermediaries, data centres, body corporate and government organisations, Virtual Private Server (VPS) providers, cloud service providers and Virtual Private Network Service (VPN Service) providers.

Types of incidents to be reported
There are 20 types of incidents that need to be reported (Refer to annexure-I for more details), including port or vulnerability scan reconnaissance incidents, as well as serious incidents such as phishing, malware, and Distributed Denial of Service (DDoS).

Timelines and how to report
Timelines: All incidents need to be reported to CERT-IN within six hours from the occurrence of the incident or of the incident being brought to the respective SPOC's notice.

How to report?
Incidents can be reported to CERT-IN via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969).

System time synchronisation
Organisations must connect to the Network Time Protocol (NTP) Server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL), or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems' clocks.

National Informatics Center(NIC): Samay1.nic.in, samay2.nic.in

National Physical Laboratory: time.nplindia.org

Setting-up point of contact
A Point of Contact (POC) needs to be designated to liaison with CERT-IN. The details of the POC need to be sent to CERT-IN in the format specified in annexure II and need to be updated from time to time. All communications from CERT-IN shall be sent to the said POC.

Recommendations to comply with CERT-IN's directive

Several steps an organisation could take to comply with CERT-IN's directive include the following:

Conduct cyber simulations
Conduct simulations that test the effectiveness of their controls and processes and identify gaps to prepare for what's coming next.

Cyber incident response
Investigate and respond to cyber incidents affecting their environment to effectively drive protection, containment, and remediation activities.

Threat intelligence
Organisations could opt for leading industry products and reliable intelligence to provide greater visibility into the evolving threat landscape.

Attack surface management
Organisations could identify risks, test swiftly, and manage the remediation of vulnerabilities identified in their environment to reduce the risk of exposure to cyber threats.

Threat detection and response
Enterprises can detect, investigate, and respond to threats based on a centralised view into activities across the network.

Threat hunting
It is essential to proactively hunt for advanced threats that evade detection by conventional security controls, to stay secure, vigilant, and resilient to any incoming attacks.

Conclusion

CERT-IN's directive is in the interest of our country's national security, as with India's growing economy, there is a greater demand for organisations to be cyber ready, to protect its people, infrastructure, and data.

Annexure I - Type of incidents that need to be reported

1. Targeted scanning/probing of critical networks/systems
2. Compromise of critical systems/information
3. Unauthorised access of IT systems/data
4. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
5. Malicious code attacks such as spreading of virus/worm/Trojan/Bots/Spyware/ Ransomware/Cryptominers
6. Attack on servers such as database, mail and DNS and network devices such as routers
7. Identity theft, spoofing and phishing attacks
8. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
9. Attacks on critical infrastructure, SCADA and operational technology systems and wireless networks
10. Attacks on applications such as e-governance, e-commerce etc.
11. Data breaches
12. Data leaks
13. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, and servers
14. Attacks or incidents affecting digital payment systems
15. Attacks through malicious mobile apps
16. Fake mobile apps
17. Unauthorised access to social media accounts
18. Attacks or malicious/suspicious activities affecting cloud computing systems/servers/software/applications
19. Attacks or malicious/suspicious activities affecting systems/servers/networks/ software/applications related to Big Data, blockchain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing,
20. Attacks or malicious/suspicious activities affecting systems/servers/software/ applications related to AI and ML

Annexure II - Point of contact information

Format for providing Point of Contact (PoC) information by service providers, intermediaries, data centers, body corporate and government organisations to CERT-IN

- Name
- Designation
- Organisation name
- Office address
- Email ID
- Mobile number
- Office phone
- Office fax

Annexure III - Details to be maintained by VPS, VPN, and cloud service provider and KYC requirement

Following accurate information must be maintained for 5 years or longer:

1. Validated names of subscribers/customers hiring the services
2. Period of hire including dates
3. IPs allotted to/being used by the members
4. Email address and IP address and time stamp used at the time of registration/ on-boarding
5. Purpose for hiring services
6. Validated address and contact numbers
7. Ownership pattern of the subscribers/ customers hiring services

Documents needed for KYC:

a. The passport,

b. The driving license,

c. Proof of possession of Aadhaar number,

d. The Voter's Identity Card issued by the Election Commission of India,

e. Job card issued by NREGA duly signed by an officer of the State Government and

f. Letter issued by the National Population Register containing details of name and address.

g. Validated phone number

h. Trading account number and details, bank account number and bank details

Annexure IV - Information security information reporting template

- Summary of incident
- When was the incident detected (provide date and time)?
- How was the incident detected?
- Which is affected by the incident, IPs or URLs?
- Details of the affected system or service (location, platform, details of security audit done)
- Details of incident investigation (if any)
- Details of mitigation action (if any)
- Details of impact
- Incident reporter (provide your name, phone number, e-mail, and address)
- Details of Contact Person for the incident (provide name, ph.no, e-mail & address)
- Any other relevant information

References

- CERT-In Direction for Incident Reporting in 6 hours
  https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
- CERT-In Incident Reporting Form
  https://nic-cert.nic.in/pdf/Information%20Security%20Incident%20Reporting%20Form.pdf
- The Information Technology Act, 2000
  https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Connect with us

Rohit Mahajan
President - Risk Advisory
Deloitte India
rmahajan@deloitte.com

Gaurav Shukla
Partner and Leader, Cyber, Risk Advisory
shuklagaurav@deloitte.com

Aloke Kumar Dani
Partner, Risk Advisory
alokekdani@deloitte.com

Anand Prakash Tiwari
Partner, Risk Advisory
anandtiwari@deloitte.com

Contributor

- Amulya Ratna

Deloitte.