SME concerns with CERT-In Directions

Recommendations on compliance timelines for SMEs and additional suggestions for improving ease of compliance

About Hasgeek

Hasgeek Learning Private Limited is a media platform company, incorporated in 2015. Hasgeek facilitates peer-reviewed conversations on technology and its impact on business and society. Hasgeek's brands include Rootconf, The Fifth Elephant, JSFoo, 50p and Privacy Mode. The current report is an outcome of the discussions held with tech leaders and senior engineers from SMEs on CERT-In's new cybersecurity directions.

Context

On 28 April 2022, CERT-In released directions for cybersecurity incident reporting. With the compliance deadline of 28 June fast approaching, industry bodies shared their concerns with CERT-In and MoS Rajeev Chandrashekhar on 10 June 2022.

At the meeting, MoS asked for suggestions for a reasonable time frame for Small and Medium Enterprises (SMEs) to comply with CERT-In's directions. Rootconf organized a meeting with representatives from SMEs on 14 June 2022 to discuss the issue of compliance timeline. **SME representatives opined that 300 days from**

28 June 2022 is a reasonable time frame for complying with CERT-In's directions.

The intention of this document is to collectively navigate through the new CERT-In directions published on 28th April 2022, with the SME community, and provide useful suggestions pertaining to the directions, such that there is ample time to incorporate them, and minimum friction in implementation. Additional suggestions that came up in the meeting are as follows:

Suggestion	Specific requests
Periodic consultations with industry bodies to discuss issues that emerge during compliance.	1. Increase clarity around logging data; both around exact data logging requirements for service providers, and the number of days that the data is to be stored, as costs increase almost exponentially with time.b. Requires external validation services. 2. On incident reporting: • Create a "good Samaritan" framework for individuals in organizations who report incidents. • Require reporting when systems are impacted due to DDoS/DoS attacks and not for every targeted scan. • Maintenance of a portal by CERT-In, with form-based submissions as a reporting mechanism to streamline the process. 3. Investigation participation of service providers, when required, over email, phone or remote video conferencing as opposed to being summoned in person. 4. Parity in compliance requests for both foreign and Indian companies. 5. Provide clarity on methods used by CERT-In to ensure security of the data they receive.
Organize training and capacity building for law enforcement officers.	1. Build knowledge around data access and sharing that are stipulated in the current sharing regulations.

Suggestion	Specific requests
	2. Manage incident reports handling of complex deployments.
Introduce certification-like approach for compliance.	1. Help organizations to implement the requirements in a more structured manner. The compliance can thus be transparently evaluated based on the requirements.
Provide a wider range of options for customer validation.	1. Aadhaar-based customer validation via services such as digio.in and bureau.id, which do not collect a copy of Aadhaar but use it for name and address verification or Aadhaar signatures through separate OTPs. 2. Vetting of third-party identity validation providers outside of India to facilitate foreign companies' and nationals' identity and address validation.

Rootconf is invested in facilitating further interactions between CERT-In and representatives from the SME community to improve the state of cybersecurity in the Indian tech ecosystem.

Acknowledgement

We thank all the participants who partici-
pated in this discussion and took the time
to comment on the new directions as well as
review and edit this document. Responses
have been anonymized as per Chatham House
Rules.

Contact details

Phone: 91–7676332020

Email: rootconf.editorial@hasgeek.com

Telegram channel: https://t.me/rootconf