Computer Security Incident Response Team in Finance sector (CSIRT-Fin)

Role of CSIRT-Fin

CSIRT-Fin is a nodal sectoral CSIRT which provides Incident Prevention and Response services as well as Security Quality Management Services to the entities of the Indian financial sector. It manages cyber incidents and coordinate responses across banking, securities market infrastructure, insurance, and pension funds entities. It carries out the following roles related to the cyber security in financial sector:

i. Collection, analysis & dissemination of information on cyber incidents.
ii. Forecast and alerts on cyber security incidents.
iii. Emergency measures on cyber security incidents.
iv. Coordination for cyber incident response activities.
v. Issue guidelines, advisories, vulnerability, and white papers relating to information security
vi. Monitor sectoral efforts in the financial sector towards maintaining dynamic and modern cyber security architecture, developing awareness amongst regulated entities and public in general.
vii. Such other functions relating to cyber security in the financial sector, as may be prescribed.

Activities of CSIRT-Fin

- CSIRT-Fin performs Incident Response (IR) activity for the financial sector. This is the core activity of CSIRT-Fin which is triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system, etc.
- Handling of security incidents in collaboration with CERT-In which include security incidents related to vulnerable services, botnets, open services, phishing, unauthorised access, etc.
- Coordination of onboarding of Financial entities to CERT-In's Cyber Swachhta Kendra (CSK) for providing automated feeds regarding malware infections, botnets and vulnerable services.
- Issuing advisories, vulnerability notes and virus alerts along with CERT-In.
- Tailored threat intelligence alerts for proactive measures are sent to financial sector constituency and entities that have been on boarded on CERT-In's threat intel platform.
- Coordination with regulators in financial sectors viz RBI, SEBI, IRDA, PFRDA, for implementation of security best practices and enforcing mandatory cyber security guidelines (for compliance)
- Interface with CERT-In for coordination of incidents involving other stakeholders like LEA, international CERTs, service providers etc. and participate in activities of cyber security assurance, implementation of Cyber Crisis Management Plan (CCMP), conducting exercises/drills in financial sector and participating in relevant forums. Interface with NCIIPC w.r.t incidents affecting notified CII in financial sector
- Provide guidance, oversight and inputs related to cyber security posture to Department of Economic Affairs (DEA), Department of Financial Services (DFS), Regulators in financial sector and MeitY under intimation to CERT-In.
- Examine trends in the cyber threat landscape.

- CSIRT-Fin, CERT-In, National Institute of Securities Markets (NISM), Information Security Education and Awareness (ISEA) and C-DAC, Hyderabad have conducted a certification program on "**Cyber Security Foundation Course**" through learning management system platform for all interested/working persons in the financial sector/ Securities Markets. (visit https://estore.nism.ac.in/cyber-security-foundation/)
- Participation in International forums like BRISC (BRICS Rapid Information Security Channel), FSB (Financial Stability Board), SIFMA Quantum Dawn, etc.
- Conduct trainings

CSIRT-Fin Contact

Address

CSIRT-Fin,
CERT-In, 1st Floor, Tower B,
DMRC IT Park, Behind Shastri Park Metro station,
New Delhi, Delhi 110053

Email: csirt-fin@cert-in.org.in