CERT-In Guidelines: Applying Key Security Procedures to Detect, Mitigate and Report Cyber Incidents

Cyber incidents and cyber security incidents have been and continue to be reported from time to time. And the complexities arising from modern-day enterprise IT set-up make it challenging to detect and respond to cyber incidents in a timely manner.

Indeed, in the backdrop of the increased pace of digitalization, businesses, organizations, and government agencies are not just witnessing a higher number of IT end users but complex IT infrastructure environments.

Today's IT infrastructure invariably includes hybrid datacentre environments, heterogeneous technologies, and distributed end users across the enterprise IT infrastructure. As a result, the IT security team often fails to detect IT anomalies in a timely manner. Adding to the challenges is the fact that far too often, organisations lack proper security mechanisms to detect and respond to threats.

The Indian Computer Emergency Response Team, or CERT-In, a statutory body under the Information Technology (Amendment) Act and a function under the Government of India's Ministry of Electronics and Information Technology, acts as a national agency in the field of cyber security.

The primary objective of CERT-In is as follows:

- Collection, analysis and dissemination of information on cyber incidents;
- Forecast and alerts of cyber security incidents;
- Emergency measures for handling cyber security incidents;
- Coordination of cyber incidents response activities;
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
- Such other functions relating to cyber security as may be prescribed.

CERT-In's latest guidelines (dated April 22nd, 2022) mandate that organisations must have the necessary mechanisms in place to gather relevant information in response to cyber incidents. Not only that, the authorities have also mandated organisations to report cyber incidents as mentioned in Annex I to CERT-In within 6 hours of notic ing such incidents or being brought to notice of such incidents.

What kind of cyber incident needs to be reported to CERT-In under Annexure I of new guidelines?

1. Targeted scanning of the critical networks/ systems
2. Compromise of critical systems/ information
3. Unauthorised access of the IT systems/ data assets
4. Defacement of website or intrusion into a website and any unauthorised/ unapproved changes done
5. Malicious code attacks such as spreading Virus/Trojan/Bots/ Spyware/ Ransomware/Cryptominers
6. Attack on servers such as Database, e-Mail, 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 E-Applications such as E-Governance, E-Commerce
11. Data Breach
12. Data Leak
13. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers etc.

14. Attacks that affects digital payment systems
15. Attacks through Malicious mobile Apps/ fake Apps
16. Existence of fake mobile Apps to deceive the users
17. Unauthorised access to the 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, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, etc.
20. Attacks or malicious/ suspicious activities affecting systems/servers/ software/ applications related to AI (Artificial Intelligence) and ML (Machine Learning)

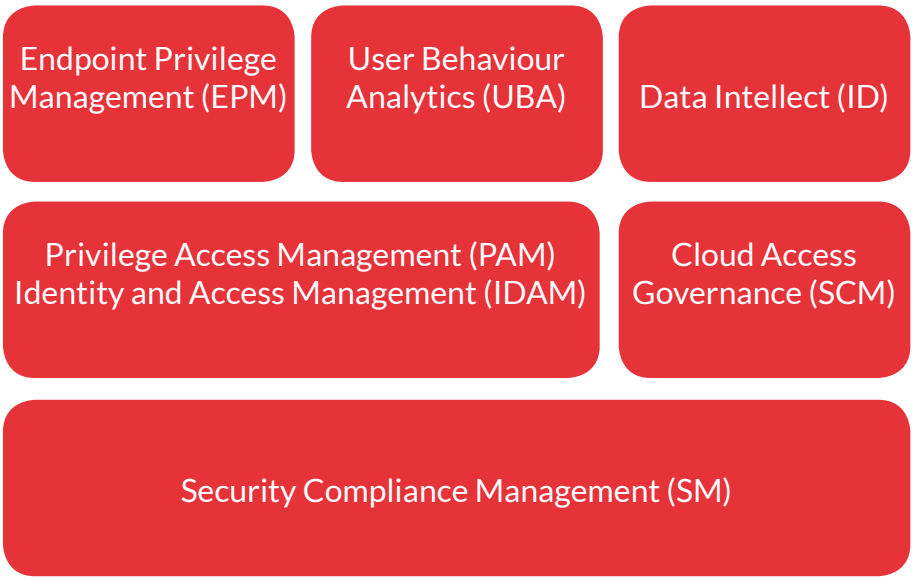
Implications of CERT-In Guidelines

Essentially, what these guidelines are requiring enterprises to do is to maintain a robust Identity and Access Management (IAM) framework, capable of providing a secure governance environment in addition to having adequate tools to detect, assess, and trigger threats on a real-time basis. Having been born out of the datacenter, ARCON understands the daily use-case challenges faced by IT teams in emerging IT environments and how to address them.

Therefore, whatever we build or innovate, the risk-predictive component is at the core. Our solutions not only prevent and protect IT threats, but predict them as well. In the next part, we will explain how ARCON's risk-predictive technologies help in building the foundation for a robust IAM architecture, which in turn helps to comply with the CERT-In guidelines.

As we explain how ARCON's robust Information Security solutions can help businesses, organizations, and government agencies timely report cyber incidents by building an IAM framework, one point needs to be reemphasized here. While these solutions will detect IT anomalies and trigger alerts on the slightest of suspicion, IT departments will have to complete the forensic assessment immediately after any alerts are raised to confirm any data breach or anything malicious in nature in order to comply with the CERT-In guidelines.

ARCON security framework to protect systems and data at every layer of IT infrastructure.



Implementing best practices in Information Security and Compliance Management. ARCON's robust stack of IT risk mitigating solutions helps to lay down the foundation for time-tested security practices. The solutions help to reinforce the data security framework at every layer of IT infrastructure and provides necessary tools to identify and raise alerts on emerging IT risks on real-time basis as well

Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In:	Solution	Benefit
Compromise of critical systems/information	ARCON I SCM	• Once ARCON I SCM is deployed, the security measures and technical configurations are incorporated at the enterprise level and applied to individual IT elements. • The solution automates the entire risk assessment process, manages execution and generates detailed review documentation of IT risk factors. Assessments can be performed for single or multiple IT elements concurrently in real time.
Unauthorised access of IT systems/data.	ARCON I PAM & ARCON I IDAM	• By implementing ARCON I IDAM, the IT risk management and compliance team can ensure that end-users' runtime access to systems is managed through a unified governing engine and every access to system is documented and reported on real time basis.
Identity Theft, spoofing and phishing attacks	ARCON I PAM & ARCON I IDAM	• While the solution's Session Management and Session Monitoring capabilities help to broker a secure session and freezes session on slightest of suspicion, the multifactor authentication (MFA) component also plays a big part in triggering alerts in case of Identity theft and phishing. • ARCON I PAM supports the following: 1.Adaptive Authentication 2.Integration with leading biometric devices 3.Standard Protocols based authentication 4.Email OTP 5.SMS OTP 6.Multiple TOPT Authenticators 7.Integration with voice recognizing authenticators 8.Integration with face recognizing authenticators

Data Breach	ARCON I PAM	• With the Incident Management feature, a privileged user is able to identify and raise an incident for any activity that looks to be suspicious.
Data Leak	ARCON I UBA & ARCON DI	• The Behaviour Analytics component detects anomalies and suspicious behaviour profiles on a real-time basis and generates risk-based scores with the help of Machine Learning and Artificial Intelligence. • The DI element is a robust DLP tool with Data Intellect that builds a contextual security layer around. DI helps in to classify data, itemize the exposed data, categorize critical and sensitive data and understand where and what of data.
Unauthorised access to social media accounts	ARCON I UBA & ARCON DI	• Granting access to social media accounts is based on the end-users' risk-based assessments. Machine Learning uses the end-users' logged data to identify risky profiles. The ML algorithms clusters risky behaviour profiles and end-user anomalies. Subsequently, the AI analytics generate a risk-score and alerts based on each end-user profile.
Attacks or malicious/ suspicious activities affecting Cloud computing systems/ servers/software/applications	ARCON I CAG	• Continuously monitors and governs identities in real time • Restrict/ allow suspicious/ authorized users at granular level • Provides Comprehensive visibility across clouds

ARCON | PAM being a highly integrable product with a capability to easily integrate with other technologies such as IGA, SIEM, OTs, RPA tools helps to mitigate and detect some of the other cyber security incidents included in Annexure I.

Conclusion

- ARCON helps organizations build a resilient IT security posture to protect confidential data
- Our robust stack of technologies helps to monitor, detect and alert IT anomalies on a real-time basis
- ARCON IAM technologies enable IT security and compliance teams to comply with CERT-In guidelines

about ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.

PAM: ARCON | Privileged Access Management (PAM) is a highly effective solution that helps in managing, controlling and monitoring privileged user activities. The solution provides IT security team with a centralized policy framework to authorize privileges based on roles and responsibilities ensuring rule-based restricted access to target systems.

UBA: ARCON | User Behaviour Analytics (UBA) is a highly effective risk predictive & analytics tool built for daily enterprise use cases. It breaks the traditional approach of 'restrictive' access and is capable of crunching large lakes of enterprise data, spot anomalous activity and trigger alerts in real-time.

SCM: ARCON | Security Compliance Management (SCM) allows an enterprise to prioritize security and compliance efforts based on risk level. The tool enables continuous risk assessment for critical technology platforms and ensuring desired compliance levels.

Connect with us