Date Updated: 17.07.2020

GUIDELINES FOR CONDUCTING CYBERSECURITY AUDITS IN THE PANDEMIC INDUCED DISRUPTION

Indian Computer Emergency Response Team (CERT-In) has created a panel of cybersecurity auditing organizations for conducting cybersecurity audits, including compliance audits, vulnerability assessment and penetration testing of computer systems, networks & applications of various organizations of the Government and those in other sectors of Indian economy.

2) COVID-19 pandemic has caused changes in workplace-culture, data flow and infrastructure at both auditee and auditing organization. These guidelines are prepared with the objective to assist auditee and auditing organizations to continue quality cybersecurity audits and address emerging cybersecurity risks due to the pandemic situation. The document is prepared after brainstorming and discussions with empaneled auditing organizations as well as key stakeholders.

3) Auditee and Auditing organizations needs to re-assess their risk profile and implement controls for minimizing the risk. Architecture changes, exposure of services, expanded organizational boundaries and changes caused due to pandemic need to be audited for security posture.

4) Services exposed on adhoc and temporary basis needs to be secured and properly audited. Such temporary changes due to the pandemic needs to be reflected in Business Continuity Plan (BCP) of organizations and thoroughly tested.

5) There is no significant impact of pandemic disruption on remote vulnerability assessments and penetration testing activities. However, conducting compliance audits and onsite audits remotely needs application of new methods and technologies.

6) Auditing as well as auditee organisation should ensure that quality of audits should not be lowered in case of remote assessment and it should replicate effectiveness of onsite assessments by use of techniques like video calling for evidence verification, asking for snapshot of command output, online interview.

7) Audits should also include expanded workplace including systems used for teleworking and connecting to organization infrastructure in audit scope. Audits of remote access policies and infrastructure needs to be performed for both auditee as well by auditing organizations (internal audits for auditing organizations).

8) Auditing organization should maintain situational awareness and their assessments should also include tests derived from recent cyber-attacks trends such as covid-19 themed cyber-attacks.

9) Auditing organizations should develop SOP for each type of audits and same should be clearly communicated to the employees and auditee organization.

10) Periodic cybersecurity audits and audits when there is change in applications or infrastructure are critical and should not be avoided or diluted.

11) Internal as well as external third-party audits are recommended for the cyber infrastructure of the organizations. To ensure independence and audits by domain experts, external audits should not be replaced by internal audits only.

12) Auditing organisations should clearly define, communicate and implement remote work policy. Also, review and mitigate the risks emerging to the IT infrastructure due to the shift in work culture (work-from-home) and technical changes in the infrastructure.

13) Process and techniques used for conducting remote audits needs to be documented in the audit report.

14) Employees deployed for audit related activities should connect to centralized server at auditing organization and all audits related activity should only be conducted by connecting to the office network. Auditors should only use office provided devices for conducting audits and these devices should only be used exclusively for audit activities.

15) Employees of auditing organizations should not connect directly to the auditee infrastructure.

16) Auditing organizations must follow secure data handling guidelines. Guidelines are available at CERT-In website.

17) Minimize the data flow outside the premises of the auditee organizations especially the data of sensitive nature should not be assessed or downloaded from outside the organizations. Techniques such as screen display through video conferencing can be used for minimizing data flow.

18) If any, data should only reside at auditing organization's servers at centralized location.

19) Communication security between auditee and auditing organizations needs to be ensured by use of proper channels and techniques of sending or sharing data and reports.

20) Audit reports, evidences and related documents should only be shared with identified single point of contact on each side through secure channels.

21) It is important to password protect the sensitive documents and share the password in a different medium from that of which the file is shared. For example, if the password protected report is shared through email, then the password should be shared through a different medium such as a SMS.

22) Auditing organizations should only provide limited access to audit related data on need to know basis.

23) Auditing organizations should implement proper controls and monitoring on data access, audit tools and related activities.

24) Non-Discloser agreements may be signed by employee of auditing organization with auditee organization.

25) Auditing organisations should ensure security of endpoints and devices used by their employees for connecting to the office environment.

26) Audits of endpoints at both auditing and auditee organisations should also include verfication of security awarness sessions for the employees.

27) Jump servers as an intermediary server through which auditing organizations can access device behind the firewall can be implemented at auditee organization. Jump server should be properly secured and monitored.

28) Auditee organizations may also whitelist only the static IP addresses listed by the auditing organization.

29) Auditee and Auditing organization should maintain continuous communication. Vulnerability scanning, penetration testing, evidence collection activities should be planned and access to auditing organization should be removed immediately after the completion of scheduled tasks.

30) Background verification of employee, documented assignment of roles and responsibilities and Do's & Don'ts document should be done/prepared by the auditing organization.

31) Auditee organizations may also consider obtaining audit certificate from critical IT or security service providers for verification of their security posture in changed workplace culture.

32) As per data security requirements, auditee may also consider providing their own laptops for assessments to auditing organization.

33) Auditee organization should know details of employee of auditing firms involved in audit activities, NDA with all deployed employees and undertaking regarding their background verification may be obtained from auditing organization.

34) Avoid confidential data sharing over web meetings and public servers.

35) Auditee and Auditing organizations should update their incident response plan with risk assessment for the new workplace culture such as compromise of WFH device, VPN breach, insider threats, leak of audit artifacts and data.

36) Auditing organisation should implement security dashboard for tracking employee activities.

37) Implement security best practices for VPN such as strong password policy, multi-factor authentication and monitoring of VPN traffic for any suspicious patterns.

38) Auditing and auditee organisations should conduct continuous monitoring of remote access logs.

39) Auditee organisation should periodically carry out data backup and test it.

40) Implement data security and encryption at auditing organizations.

41) Auditing organisations should ensure to hardening of the end-point systems, regular updates and patching, security of VPN and web meeting tools.

42) Work-from-home related functionalities should be covered under security governance and continuous security monitoring activities by both Auditing and auditee organisation.

43) Auditing and auditee organisation should apply appropriate security controls and technologies such as mobile device management, BYOD monitoring, Data Leak Prevention to counter the perceived risk.

44) Guidelines from CERT-In website such as guidelines for Desktop Security (www[dot]cert-in[dot]org[dot]in /PDF/Desktop_security.pdf), Mobile Phone Security(www[dot]cert-in[dot]org[dot]in /PDF/Mobile_phone_Security.pdf), Broadband Internet Security (www[dot]cert-in [dot]org[dot]in /PDF/Broadband_Security.pdf) and USB Devices Security (www[dot]cert-in [dot]org[dot]in/PDF/USB_Security.pdf) could be used for preparing awareness guidelines by the organizations for protecting end user systems.