Cybersecurity Blog

Everything about threat intelligence, blue team, red team, pentesting, security audit, security review, testing and assessment.

Sunday, November 24, 2019

Guidelines for Corporate Email Audit

Many security firms often provide audit assurance to their clients. As a part of their many activities, auditing corporate email system is one of their principal activity. In this article, I have 40 guidelines which an auditor or manager can use to audit their clients' corporate email system. It includes some technical and more procedural guidelines.

1. Understand who is authorised and unauthorised to send and receive documents and sensitive messages through an email system.
2. Check whether 2FA is enabled or forced to all users to access their email account.
3. Check whether passwords are changed periodically or not.
4. Determine whether email system access is segregated from other systems such as applications, databases etc.
5. Check how emails are stored on a server, what are backup policies and plans for email archives.
6. Are email archives restorable?
7. Are email archives stored encrypted?
8. Check whether the person is required email access aligned to his/her job role. Make sure policies are established for the same, including job roles, level of access, etc.
9. Monitor all outgoing emails on external domains.
10. Process of creating email accounts must be well documented, monitored and aligned with all security policies, procedures and approvals.

11. Determine any personal use of a corporate email account.
12. Implement an email privacy policy.
13. Ensure the usage of pretty good privacy (PGP) security program.
14. Check whether the email system provides default password to all new users. If yes, then is there any mechanism to change the default password or are users forced to change their first default password? Also, ensure password strength policies.
15. Webmail access must be restricted to IPs.
16. Enable blacklisting policy.
17. Check the authorisation level of printer access to all email documents printing by each user. Are they allowed to print documents from email?
18. MDM must be implemented for mobile email usage.
19. Disable email relays to prevent unauthorised access.
20. Ensure administrator account for email gateway is secured with 2FA and strong password.
21. Ensure physical security implementation to deny physical access of email server/system.
22. Email usage policies are written, circulated and communicated well. Monitoring of standard email usage practices must be taken care of.
23. Legal disclaimer should be written in every email by default.
24. Secure mail clients using patches and latest versions of upgrades/updates.
25. Provide security awareness training to employees and contractors.
26. Harden mail server application.
27. Log everything.
28. Mail server should be located in DMZ.
29. Mail server should be protected by firewall, IDS, IPS.
30. Ensure email systems are protected against ransomware, worms, malware, PUPs, viruses and other security threats on both host level, gateway level and application level. End-point protection systems must be deployed on the email servers.
31. Ensure all sensitive emails are encrypted.
32. Limit file size and file types on email attachments.
33. DLP must be implemented to protect data leakage.
34. Email gateway must check for malicious attachment by its own internal anti-virus/anti-malware protection.
35. Spam filtering mechanism must be in an email.
36. Enable SPF to prevent email spoofing.
37. Enable DKIM to ensure emails are trustworthy.
38. Enable DNSSEC to prevent unauthorised DNS modifications.
39. Ensure security of email system/server in the planning phase, deployment phase, installation phase.
40. Secure email server operating system by using effective patch management processes, removing running unnecessary services, hardening, security testing.

Posted by Frogy at 11/24/2019

▶ 2013 (58)

Labels: audit, compliance, corporate email, email, email encryption, mdm, o365, security

1 comment:

Cyber Security Course said...

very informative post thanks

January 13, 2020 at 12:19 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)