|  |  |  |
| --- | --- | --- |
| Asset | Configuration | Guidelines |
| Admin web app | Anti-virus with updated virus definitions | Default password should not exist. If exist, change the password during access providing |
|  | Deployed (V&V) secure system configuration model | Set your spam filters setting options to high |
|  | Statefull firewall |  |
|  | Configure firewalls to reject any packets with spoofed addresses. |  |
|  | Ignore/Delete any request seeking for personal info from 3rd parties |  |
|  | Disable device network discoverable |  |
|  | Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present |  |
|  | Restrict the system getting connected to unauthenticated sources |  |
|  | Restrict the system in accessing the 3rd party sites, social engineering sites, mails, etc.. |  |
| Azure portal administrator | Audit/system log:  All the information needed for identifying the threat (malicious) activity and adversary information needed to be logged for determining the attack vector and attack surface. This helps to make the system less vulnerable in future by correcting those issues. | Limit on logon attempts(no.) |
|  | Authentication flow diagram (secure communication) | Error messages info |
|  | Block the access to a machine (either remotely/locally) for administrator-level accounts | Multifactor authentication |
|  | Audit/System log should be secured from unauthorized access. | Default password should not exist for any assets (such as applications, operating systems, routers, firewalls, wireless access points). If exist, change the password during access providing |
|  | Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) | Limit authentication attempts (rate Limiting) |
|  | Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) | Strong password strength & Strong password policies (ex:Combination of caps letter, number, spl char...) |
|  | Stronger authentication methods |  |
| Azure cloud Database |  | Limit on login attempts |