|  |  |  |
| --- | --- | --- |
| Asset | Installation manual | Instruction manual |
| 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 | Ignore/Delete any request seeking for personal info from 3rd parties |
|  | Statefull firewall | Disable device network discoverable |
|  | Configure firewalls to reject any packets with spoofed addresses. | Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present |
|  |  | Set your spam filters setting options to high |
|  |  | 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. | Authentication flow diagram (secure communication) |
|  |  | Limit on logon attempts(no.) |
|  |  | Error messages info |
|  |  | Multifactor authentication |
|  |  | Block the access to a machine (either remotely/locally) for administrator-level accounts |
|  |  | 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 |
|  |  | Limit authentication attempts (rate Limiting) |
|  |  | Strong password strength & Strong password policies (ex:Combination of caps letter, number, spl char...) |
|  |  | Audit/System log should be secured from unauthorized access. |
|  |  | Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) |
|  |  | Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) |
|  |  | Stronger authentication methods |
| Azure cloud Database |  | Limit on login attempts |