Quality Controls

Steps of Procedure and Usefulness

Version 25.06 and latest

Dear Customer/End-User/Channel-Partner/Distributor/Vendor/Reseller and Associated.

Threats can be avoided by having proper systems / policies / process placed in a secure Network Infrastructure. It is very important to ***protect your workforce*** and systems proactively in a Centralised / Distributed business model.

Hence requesting you to please see wherever you can apply the below best practices / ***recommendation*** for products deployment onsite.

1. Server/Network device password :

- ✓ Use hard-to-guess passwords or passphrases.
- ✓ Use different passwords for different accounts.
- ✓ Change password after every 30-45 days.
- ✓ Administrator password/rights should only be with 1-2 persons.
- ✓ Two factor authentication is usually recommended.
- ✓ Use recommend tools like, Privileged identity management.

2. Vulnerable ports :

- ✓ Do not allow vulnerable ports access to any IP or users.
- ✓ Do allow limited IP or users access to required ports.
- ✓ Do set up firewalls and do not allow any/all rules.
- ✓ Do have strong firewall policies.
- ✓ Do set dedicated settings for NMS / Automation devices with strict permitted rules.
- ✓ Do set usage of end points encryption and UTM services.
- ✓ Do set IPSec for Critical mission devices/network/appliances.

- ✓ Do not allow unsecured physical access within DC/server room facilities.
- ✓ Only authorised personnel should be allowed through proper authentications.

Common vulnerable ports are as mentioned below:

Unsecured / Vulnerable Ports	Port No	Secured Ports	Port No
FTP	21	FTPS	990
Telnet	23	SSH	22
SMTP	25	SMTPS	465 / 587
DNS	53	DNSSEC	53 (with validation)
HTTP	80	HTTPS	443
IMAP	143	IMAPS	993
NETBIOS	137-139	POP3S	995
MSSQL	1433-1434	MS-DS (Kerberos/LDAP over TLS)	3269
PPTP	1723	RDP (with TLS)	3389 (TLS enabled)
MYSQL	3306	VPN / IPSec	500 / 4500
RDP	3389	–	–
VNC	5900	–	–
HTTP-PROXY	8080	–	–
RPCBIND	111	–	–
Win RPC	135	–	–

3. Anti-Virus Policies :

- ✓ Have anti-virus software installed and keep it updated with latest patches.
- ✓ Have anti-virus scan done frequently.
- ✓ Antivirus scanning is recommended to be done during non-business hours.
- ✓ Have your IT infra updated with latest OS and security patches.

4. Backup :

- ✓ Do Backup your files on regular intervals.
- ✓ Backup is recommended to be done during non-business hours.
- ✓ Do not keep backup and business applications on same system/server.
- ✓ Update save-sets/backup folders as and when required.
- ✓ Monitor the backup report and act wherever necessary.
- ✓ Do mock drills of data restoration on regular intervals.

- ✓ We recommend high availability setup (HA) infra.
- ✓ Do mock DR drills on regular intervals.

5. Employees Policy :

- ✓ Do train employees on cyber security and outline company policies.
- ✓ Employee access and exit policy should be strongly followed.
- ✓ Do install and update antivirus on your office desktops and laptops.
- ✓ Limit USB access to office desktops and laptops.
- ✓ Password sharing among peers is a crime.
- ✓ Do not open mail or attachments from an untrusted source.
- ✓ Limit installation of unauthorized applications or Software.
- ✓ Limit employees from accessing unauthorised websites.

6. ToT (Transfer of Technology):

- ✓ Do report all suspicious activity and cyber incidents to your IT Admin/Concern officer/Management.
- ✓ In-house tampering at offline infrastructure is sole responsibility of End User Organisation.
- ✓ Un-authorised Reverse Engineering is only complied if written to share ToT (Technology of Transfer) officially.

For any support related to our products

Raise TAC / RMA – www.akus.co.in (write us: support@akus.co.in), For consultation: sales@akus.co.in. Talk to us:- **1800 309 9987** (Toll-Free)

Please give us feedback on this learning guide, so we can provide content that's truly useful and helpful. Thanks!

Regards,

AKUS Team