

Security Practices – Critical Checklist

Business Risk Assessment – Critical Asset Protection

Identify most critical systems; ensure they are given the highest priorities for all hardening and monitoring activities

Active Directory and Exchange Hardening

- Minimize number of admins
- Monitoring and alerting (Windows Event ID #566)
- Two factor admin access from hardened VDI platform
- Executable whitelisting on hardened DCs
- Disable default account and rename key accounts
- Complex passwords (9 & 15 Char)

Infrastructure & Logging

- Full and detailed logging & analysis
- Tighten VPN controls
- Increase controls on crypto keys
- Full packet capture at strategic network locations
- Network segmentation
- Team trained and focused on APT activity

Service Accounts

- Review accounts for privilege creep
- Change passwords frequently
- Do not embed credentials into scripts
- Minimize interactive login
- Restrict login only from required hosts

Web Access

- Block access to high risk and web filter categories
- Click through on medium risk websites
- Black hole dynamic DNS domains
- Authenticated internet access
- DNS traffic analysis

User Education

- Increase security training for IT
- Launch security improvement initiative
- Regular education of users on phishing attacks
- Regular education on social engineering
- Increase mail filtering controls

User Machine Hardening

- Limit local admin and randomize PW- change often
- Increase patching regime
- Enable security controls in applications
- Deep visibility to identify lateral movement
- Limit use of non-authorized and unapproved software