JANUARY 2024
BULLETIN #4

SYSTEM SECURITY STANDARDS GUIDELINES FOR CYBER QUOTES

As the cyber insurance market continues to change, we have updated this summary of system security standards needed by the marketplace to obtain a quote.

MFA 100% IMPLEMENTED FOR REMOTE ACCESS AND PRIVILEGED USER ACCOUNTS

Minimum: MFA implemented for access to email (e.g. enforced via Office 365. Note, if using O365, enabling Advanced Threat Protection is also a recommended standard)

- Minimum: MFA enforced for access to "privileged user accounts" (i.e., the information technology department)
- MFA enabled for all remote access to the insured network

END-POINT PROTECTION, DETECTION, AND RESPONSE PRODUCT IMPLEMENTED ACROSS ENTERPRISE

Minimum: an End-Point Protection (EPP) solution in place

- Preferred: an End-Point Detection & Response (EDR) solution in place (Now considered a minimum on medium-large sized organizations)

IF REMOTE DESKTOP PROTOCOL CONNECTION ENABLED, THE FOLLOWING ARE IMPLEMENTED

Minimum: MFA-enabled VPN is used for access to any Remote Access software

- Network level authentication enabled

BACKUPS

Minimum: Regular backups are (i) in place, (ii) successful recovery is tested, (iii) backups are stored separately (i.e. 'segregated') from the primary network, (iv) encrypted, and (v) protected with anti-virus or monitored on a continuous basis

- Tested at least twice per year
- Ability to bring up within 24–72 hours — less time for critical operations (4–8 hours)
- Consider an offline, offsite, or secondary back up to have an additional copy of your data easily accessible for restoration purposes

PLANNING & POLICIES

Minimum: Tested and rehearsed

- Incident Response Plan
- Disaster Recovery Plan
- Business Continuity Plan
- Asset Management

ASSET MANAGEMENT

- Monitor all assets' life cycle from new asset creation to the point that it become obsolete and must be disposed of
- Ensure that cyber assets remain secure and compliant
- Spot unknown assets and bring under management for their protection
- Regularly maintain assets to detect unauthorized changes
- Gain insight into your internal and external attack surface

TRAINING

Minimum: Training and regular simulated phishing exercises for all users

- Social Engineering Training
- Phishing Training
- General Cyber security training
- Training of account team staff on fraudulent transactions

PATCHING

Minimum: Critical & high severity patches installed within 30 or fewer days, optimally within 1–7 days for critical & high severity patches regarding active exploits

END OF LIFE SOFTWARE

- Formalize a roadmap for addressing end of life software concerns in the environment
- Provide a status update at time of submission
- All end of life devices should have a formalized roadmap for sunsetting/decommissioning, and in the interim, extended support should be purchased and access restricted as much as possible using ACL's, VLAN's, bastion/jump hosts, etc.

SERVICE ACCOUNT MANAGEMENT/DOMAIN ADMINISTRATOR ACCOUNTS

- Service account passwords should be longer than standard user accounts. Insurers recommend at least 25 characters or greater and rotated on a regular basis
- Where possible, remove domain admin privileges and disable interactive login
- Domain admin accounts should be restricted to only domain controller activity and monitored for any activities outside of that function

MISCELLANEOUS

- Sufficient IT Security budgets and dedicated security personnel, carrier generally like to see 10% of total IT spend go to security but this will differ based on organization size
- Email security controls in place
- Privileged Access Management. A PAM solution is now considered a minimum on medium-large sized entities
- Consider implementing system monitoring 24/7 to check the condition of your IT infrastructure in real time
- Establish a formalized enterprise risk register as well as third party management

- Please note this list is context dependent. If an underwriter views a client as potentially higher risk (e.g., due to previous incidents/losses) then they may look for more controls beyond the 'minimums'
- If the market continues to harden, underwriters' 'minimum' expectations may increase
- Different insurance carriers may have different expectations of 'minimums'. This is our current best understanding
- Many carriers are no longer writing new Public Entity business, regardless of controls