TIPS FOR BUILDING AUTOMATION CYBER SECURITY

The following are some cyber security tips to consider as your team designs and develops building automation systems.

1. Design hardware and software to be more easily patchable and updatable, both by the manufacturer, and locally by the owner where the owner won't permit the manufacturer to have remote access.
2. Improve controls on who has access to the software ("priority access management")
3. Passwords
    - A. Don't use same password for different devices
    - B. Require default password to be changed on installation
    - C. Unique password for every device leaving the factory (no default password)
    - D. Never store passwords in clear text; encrypt them
    - E. Improve password encryption
    - F. Reduce leakage of password info
    - G. Change periodically
        - i. After initial install
        - ii. After key employee leaves
        - iii. Periodically
4. Use 2-factor authentication in software for access by remote contractors
5. Use software security scanning to find vulnerabilities before it is released. Require software/chip vendors to do this and verify.
6. Implement IP address restrictions
7. Routers:
    - A. Disable remote admin feature
    - B. Close ports that don't need to be open
    - C. Monitor network activity between routers, automation systems and embedded devices
8. Segmentation of systems to prevent leaping over firewalls. Have infrastructure network be different than the corporate network.
9. Financial controls: have changes in financial account info for vendors vetted:
    - A. Call the vendor
    - B. Do a test wire of $100 to make sure it went to the right bank account
    - C. If wire fraud, contact the FBI within 48 hours: "Financial fraud kill chain"
10. Employee training
11. It is key for real estate and IT to be on the same page on protocols, processes, and approvals for applying new technologies.
12. Include IT and security individuals as part of the construction design team
13. How do you handle announcing a patch after you discover and/or fix a vulnerability?
14. Need to protect data and systems':
    - A. Integrity
    - B. Availability

C. Confidentiality

15. Device security tips
    A. Authentication of device before being integrated into the network
        i. avoids spoofing
    B. Verify and authenticate source of the device's software (digitally signed by vendor ["trusted source"])
        i. Unsigned software may be compromised
    C. Patching/updating
        i. Done in a way that doesn't compromise device operation
        ii. Only from authenticated sources
        iii. Done in a way to minimize risk of losing data or interfering with operations,
        iv. verifying that update was performed before putting back online
    D. Access control
        i. Least-privilege access. Access levels:
            (1) Querying state
            (2) Updating software
            (3) Changing configuration
    E. Design IOT software analytics to be able to detect anomalies
        i. Higher than expected traffic may be a sign of compromised system
        ii. Abnormal access times or patterns
16. Review and update your reseller, partner, customer, and other agreements to ensure you have minimized your risk and liability.

If you have any questions, please feel free to contact me.

BARNES & THORNBURG LLP

Jason A. Bernstein
Phone: (404) 264-4040
jason.bernstein@btlaw.com

Barnes & Thornburg LLP
3340 Peachtree Road, N.E.
Suite 20900
Atlanta, Georgia 30326
www.btlaw.com

Partner

- Data Security & Privacy (Group Co-Chair)
- Technology Agreements
- Intellectual Property