Cybersecurity Concerns in Building Automation

September 2023

First Let’s Examine Common Network Configuration Theory

- 99%+ of all networks are designed to be Perimeter Networks
- This is based on 20-30 year old networking concepts and has some serious flaws!
    - All computers, servers, printers, devices etc. are allowed to communicate with each other openly via TCP/IP or other protocols.
    - This makes it very easy to have a single infected device outbreak an infection across the entire network!
    - This allows hackers to run C&C within your network totally unchecked.
    - Network configuration enumeration is very easy as well!

Common Software and User Policy Issues

- Can anyone here tell me every single piece of software running on their network right now? What version? Who is or isn’t running it?
- What about network protocols? Can you tell me every single one your automation uses?
- We are totally clueless as to these answers beyond common basics!
- Does anyone here have an employee in their company that is required to work 24 hours a day?
- We give users an unprecedented amount of access to the network, and we usually don’t think about it!

The Next Generation of Network Design: Zero Trust

- Brief history: This network model was created in 2010 by Forrester Research and is currently the network design of choice for cybersecurity and cyberwarfare.
- Zero Trust is data centric and has three key concepts:
    - Ensure all resources are accessed securely regardless of any location (we assume ALL traffic is threat traffic until validated, inspected, and authorized)
    - Enforce Access Control with the Least Privilege Principle in place (eliminates the human temptation of accessing things they shouldn’t)
    - Inspect and log ALL traffic (verification of Digital Identity)
- TRUST BUT VERIFY IS OLD THINKING!!!

Zero Trust Execution Concept: Segmentation

- Create micro-perimeters within your internet/firewall/router perimeter.
- Depending on availability of bandwidth performance these perimeters can be larger than 1-to-1 to start but shouldn’t stay that way.
- Each micro-perimeter can be virtual segmentation, physical, or programmed non-routable for older devices or computers.

- The goal here is to only allow computers/servers/devices access to the resources they need!

Zero Trust Execution Concept: Threat Management

- Micro-perimeters within the LAN should ALL be routed through a Next Generation Firewall (NGFW).
- An Enterprise level firewall has the following critical features:
    - Unified Threat Management (UTM)
    - Zero Day Updating with Sandboxing for known threats
    - Coverage for mobile devices (VPN or CASB)
    - SSL/TLS Decryption (you miss ~50% of traffic without this!)
    - Application Whitelisting
    - Windows Login integration
- DO NOT CHEAP OUT ON THIS!!

Zero Trust Execution Concept: SIEM

- Security Information and Event Management (SIEM) is the fastest way to understand problems and threats within your network!
- SIEM has the following capabilities/components:
- Data aggregation (pulling logs from multiple sources)
- Correlation (helps to link potential threats and problem across multiple systems)
- Alerting
- Dashboards for easy monitoring and management
- Compliance (automate compliance/auditing data for reporting)
- Retention of data for analysis on APTs
- Forensic Analysis utilities
- SOC MONITOR THE SIEM!!!

Enhancing Zero Trust in the Future: Software Defined Perimeter

- SDP is a concept that began its development in 2013 and by 2025 is expected to be standard for remote access, displacing previous models such as VPNs.
- First, SDP verifies incoming data requests to the network using three different methods:
    - Verification of the User's Identity
    - Verification of the device the user is connecting with
    - Verification of their role within the organization
- Second, SDP creates a unique cryptographic verification to ensure the first point is valid and secure.
- Leveraging the cloud is the easiest way to achieve this, thanks to Cloud Access Security Brokers or CASB
- Finally, the SDP connection must verify that the protocols used to achieve the connection are proven to be correct through the use of public domain security controls.

Your Existing Network of Automation: Advanced Security Policies

- Enforce good password policies!
- Enable MFA wherever possible (Remote logins to your automation, desktop logins, websites, cloud, everything possible!).
- Limit access logon hours.
- Limit access to critical computer functions like Control Panels, application install/remove features and more.
- Limit access to needless data removal methods like USB drives, Dropbox etc.! Your customized automation configurations shouldn't get out there!

Your Existing Network of Automation: Proactive Defense Measures

- Use and enforce a monitored patch management system like a Remote Managed Monitoring or RMM. Don't let your automation setup go unpatched!
- Review configurations and products for existing automation defenses like firewalls and threat detection.
- Schedule and perform periodic penetration testing to ensure your defenses remain hardened (usually quarterly for this unless you're massive!).

Your Existing Network of Automation: Improvement Planning

- Improvement planning is not only for recovering from a disaster!
- Your company should have a quarterly and annual improvement plan that is no more than two years in total.
- Perform a Cybersecurity assessment on your IoT and automation based on a Cybersecurity Framework like NIST SP 800-213.
- Set a proper and accurate budget.
- Understand how your cybersecurity improvements help your customers' security, and don't forget to tell them that in marketing/sales!

Quick Tech Review: Foundational Defense for On-Site Automation and IoT

The Critical Components for Cyberdefense

1. Next Generation Firewalls to create a perimeter and isolate your IoT
2. Next Generation Threat Detection for computers controlling the IoT
3. Enterprise Level switches and wireless access points to achieve isolation
4. 24/7 SIEM/SOC Monitoring for all of the above
5. Encryption systems (at rest and in transit)
6. Awareness and Training Programs for technicians with access

What this doesn't cover is everything beyond the technical solution such as asset management, policies, processes, etc.

Things You Can Start Doing Right Now!

- Start with a Cybersecurity Risk Assessment and Audit. This isn't quick!
- Continuously monitor for patching and updating.
- Verify configurations are accurate and secure.

- Review your passwords ASAP.
- Enable free Multifactor Authentication options until you adopt a corporate solution.
- Firewall everything you can!
- Protect mobile devices via free options like encryption until you adopt a corporate solution.
- Have the right IT staff, outsourced or internal. IT is NOT Cybersecurity!
- Start educating all users and adopt a training platform.

About Nick Espinosa

Chief Security Fanatic at Security Fanatics

An expert in cybersecurity and network infrastructure, Nick Espinosa has consulted with clients ranging from small businesses up to the Fortune 100 level for decades. Nick founded Windy City Networks, Inc in 1998 at age 19 and was acquired in 2013. In 2015 Security Fanatics, a Cybersecurity/Cyberwarfare outfit dedicated to designing custom Cyberdefense strategies for medium to enterprise corporations, was launched. A internationally recognized speaker, member of the Forbes Technology Council, TEDx Speaker, strategic advisor to humanID, regular columnist for Forbes, award winning co-author of a bestselling book "Easy Prey", host of "The Deep Dive" nationally syndicated radio show, on the Board of Advisors for Roosevelt University's College of Arts and Sciences as well as their Center for Cyber and Information Security, the President of The Foundation for a Human Internet and is the Official Spokesperson for the COVID-19 Cyber Threat Coalition. Nick is known as an industry thought leader and sought after for his advice on the future of technology and how it will impact every day businesses and consumers.

Keep Up with the latest in Cybersecurity at:

https://twitter.com/NickAEsp
https://www.facebook.com/securityfanatics
https://www.linkedin.com/company/securityfanatics
http://www.securityfanatics.com