Cybersecurity Concerns for Electrical Contractors
September 2023

Demystifying the Dark Web

- The Dark Web can be monitored for immediate remediation!
- Stop using corporate email addresses for logins outside of corporate needs.
- Using complex passwords goes a long way to protecting your data.
- Multi-Authentication (MFA) with Identity Management is your best friend.
- Filtering employee's website access ensures sites are safe to browse.

Cloud Security Made Easy!

- Ensure that your cloud developers are certified professionals for the cloud platform they're developing on.
- Have a third party check your cloud configuration settings.
- Running periodic penetration tests ensures security.
- Patch your cloud infrastructure regularly and immediately.
- Install a Web Application Firewall (WAF) or Next Generation Firewall (NGFW) in front of your cloud infrastructure to prevent hacking.
- Enable MFA on your users and administrative consoles.

Network Design Done Right

- Zero Trust Networking Access (ZTNA) is your new best friend and will stop infection outbreaks and hacking.
- Software Defined Perimeter (SDP) or Cloud Access Security Brokers ensure that Devices and Identities are verified before allowing to connect.
- Buy the right hardware (not all are built the same even if they're the same on paper!).
- Monitoring critical infrastructure for threats and immediate remediation.
- Isolate remote and mobile devices from the network.
- Enabling User Policies that remove needless choices from users.

Defending Your Mobile Devices

- Encrypt ALL mobile devices (phones, laptops, tables) to protect data against lost or theft. Ideally AES256 based encryption.
- Use a modern CASB (or VPN if that's the only option) that not only encrypts your phone's data but also puts it behind a Next Generation Firewall for advanced threat protection.
- Kill BYOD policies if you can.
- Use Mobile Device Management (MDM) platforms to enforce all of the above and restrict use such as app installations and web browsing.

Education the Masses

- Regular awareness training can be automated and gamified.
- Create user policies that enforce corporate policies for technology such as:
    - Internet usage (i.e. no Facebook or limited ability to browse).
    - Remote access policies that are secure and limited in scope.
    - Limits on using personal technology such as laptops, flash drives and phones.

Understanding Roles of Your Technical Staff

- Non-Technical Executive Leadership usually has no idea regarding technical roles, to the company's detriment.
- IT Staff is NOT Cybersecurity Staff!
- Misconfigured Cyberdefense is usually the result of well-meaning IT personnel with a lack of Cybersecurity training and education.
- Poor choices can cost company millions financially and harm reputations!

A Basic Risk Framework to Get You Started!

- When a company has zero understanding of their Risk or Risk Quantification, we usually start with this equation:
    - Cyber Risk = Threat x Vulnerability x Information Value
- Basically this breaks into:
    - What is the threat?
    - How vulnerable is the system and current processes?
    - What is the reputational or financial damage if the system is breached or made unavailable?
- From there, the recommendation is to do a cyber risk and cybersecurity audit using a framework like NIST 800-171.

Understanding Cybersecurity Concepts and Frameworks

- The C.I.A. is your best friend! Here's why:
    - Confidentiality – preserving authorized restrictions on access and disclosure, which includes means for protecting personal privacy and confidential data.
    - Integrity – guarding against improper data modification or destruction and ensuring data accuracy and authenticity.
    - Availability – ensuring timely and reliable access to confidential data.
- THE GOAL HERE IS TO FOCUS ON AND PROTECT THE DATA!

Understanding Cybersecurity Concepts and Frameworks Cont.

- We execute the C.I.A. through the Safeguards Method.
- The Safeguards, or Controls, are designed to look at an organization holistically from three primary aspects:
    - Technical – the technology, and its policies and procedures for its use, that is in place to defend confidential data as well as to control access to it.
    - Physical – the physical measures, as well as the policies and procedures, used to protect confidential data from unauthorized physical access and also protection from natural and environmental hazards.
    - Administrative – the maintenance, policies, and procedures with regard to the security measures that protect confidential data.

Knocking out 95% of IT – Cybersecurity Framework

- Understanding the concept of data security via C.I.A. and the practical knowledge of how to safeguard it we can now build a framework!
- The most universally used Cybersecurity Framework is NIST 800-171.
- NIST, while US based, is accepted worldwide by corporations and other governments as a model for Cyberdefense.
- Other major frameworks like CMMC, PCI DSS, and CIS are at least partially, or fully, based on NIST's fundamentals.

Core Tools and Strategies for Defending Your Company!

- Role Based Awareness Training for ALL employees
- Multiple types of backups!
- Next Generation Firewalls
- Endpoint Detection Response platforms
- Cloud based Spam Filtering
- Identity Management
- Digital Rights Management (DRM) / Data Loss Prevention (DLP)
- Cloud Access Security Broker (CASB) to replace remote access
- Contingency Planning
- Good network policies like passwords, PowerShell, access, MFA etc.
- Live Security Monitoring, Remote Managed Monitoring, Mobile Device Management, Dark Web Monitoring
- GET CYBER INSURANCE!

What You Can Do Right Now!

- Review your overall network design with your technical staff, ideally with Cybersecurity personnel.
- Conduct a Cybersecurity Assessment with Penetration Testing to understand current vulnerabilities for the network.
- Enable free security options you may not be using already such as MFA.
- Create a timeline for strengthening your defenses.
- REMEMBER: EVERY LITTLE THING YOU DO ADDS UP AND MAKES YOU MUCH MORE SECURE!

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