OCTOBER IS CYBERSECURITY MONTH

SEE YOURSELF IN CYBER

alpha TECHNOLOGIES

ARTICLE HIGHLIGHTS

1. NETWORK SEGMENTATION
2. LEAST PRIVILEGE
3. CONTINUOUS MONITORING
4. ENDPOINT PROTECTION & FIREWALL

WEEK 5: SECURING CRITICAL INFRASTRUCTURE

Welcome back to our 5th and final blog post for this years Cybersecurity Awareness Month! This week we will be focusing on ways to secure critical infrastructure. From our healthcare systems to our energy and oil sectors, these resources are necessary to keep a country going and protecting them should be an utmost priority.

CONTACT US

304-201-7485

salesgroup@alpha-tech.us

www.alpha-tech.us

Hurricane, WV

1.) NETWORK SEGMENTATION: Ransomware is on the rise and one of the main targets of interest are healthcare systems. Information such as health records are profitable for bad guys on the Dark Web and can be sold for a high price. A great way to mitigate a ransomware attack is to segment the network. By segmenting a network, it makes it harder for malicious programs to move across different devices and infect them. Think of this like a house with different rooms representing different network segments. If you don't have access to the room, then you don't have access to the contents within it, like a computer or server.

2.) LEAST PRIVILEGE: Just because an infrastructure's perimeter may be secure doesn't mean its internal network is safe. If a hacker were to find a vulnerability to get into a user's account with full permissions, they would have full access to all the data within the organization, such as a financial institution. One way to alleviate this is to ensure user accounts only have access to information and applications that are necessary for daily work. This can prevent hackers from running rampant in a network if they get into a user's account, and prevent them from transferring out mass amounts of data.

3.) CONTINUOUS MONITORING: Our nation's critical infrastructures not only rely on informational technologies (IT), but also operational technologies (OT) such as hardware that manage pipelines, generators, cooling systems, etc. If malicious actors were to break into a network and take control or disable OT devices, then that could lead to catastrophic consequences. Continuous monitoring can help detect security activities and external or internal attacks by using automation technology like a piece of security software to constantly analyze networks and devices. With continuous monitoring in place, a hacker's attack can be foiled before they even break into a network and have the chance to wreak havoc on IT and OT devices.

4.) ENDPOINT PROTECTION AND FIREWALL – Remembering the fundamentals of cybersecurity can prevent many cyber attacks into our infrastructures. Two important things that can help our critical systems include making sure all that devices have endpoint protection and having a firewall at the perimeter of the network. These defensive tools prevent many malicious actors from stealing data or hijacking equipment, with the firewall stopping hackers at the edge of the network and the endpoint protection catching something the firewall might miss.

With that being said, this wraps up this years Cybersecurity Awareness Month blog posts. We hope that you enjoyed these helpful tips to remain secure online in both your personal and professional life. Stay safe everyone!

SECURITY OPERATIONS CENTER

CRIME HATES SECURITY; WE DON'T.

CALL TODAY FOR YOUR FREE SECURITY ASSESSMENT

304-201-7485 OPT 2