CYBER ESSENTIALS
Your success depends on *Cyber Readiness*. Both depend on *YOU*.
September 29, 2020

ESSENTIAL ELEMENT: YOUR SURROUNDINGS

THE TASK : Ensure Access Only to Those Who Belong on Your Digital Space

The access you grant employees, managers, and customers into your digital environment needs limits, just as those set in the physical work environment do (i.e., access to what's "behind the counter" or business records). Setting approved access privileges and establishing your operational procedures requires knowing who operates on your technology and with what level of authorization and accountability. User and Access Management is a complex activity and there is no one size fits all solution. Adopt a strategy appropriate to your organization and leverage a staged approach.

Essential Actions

✔ *Actions for Leaders* ✔ *Discuss with IT Staff or Service Providers*

Learn who is on your network. Do you know who is accessing your network? Do they have the proper permissions? How are they accessing your networking, and through which entry points? Create an inventory of connected devices to track who and what is on your network (i.e. Computers, smartphones, printers, and routers). Use network inventory spreadsheets to enhance security by keeping you aware of unauthorized use. Monitor and analyze user activities for anomalous behavior such as access attempts outside of normal operating hours or from unusual locations.

Resources for Taking Action

NSA Actively Manages Systems and Configurations: *a guide that offers a range of techniques to minimize mission impact.*

NSA Defend Privileges and Accounts: *designed to limit exploitation and insider threat.*

Global Cyber Alliance: *a guide and checklist to identify and secure your devices and applications.*

Center for Internet Security Control 4: *this guidance focuses on the processes and tools used to control the assignment of administrative privileges.*

Center for Internet Security Control 9: *this guidance focuses on managing operational use of ports, protocols, and services on networked devices.*

Leverage multi-factor authentication for all users. Strong access protection includes two or more factors: knowledge, possession, and inherence. Knowledge factors are something the user and only the user knows and include passwords, or personal identification numbers (PIN). Possession factors are something the user and only the user has, which can be a security badge, SMS text message with a code, and soft or hard token. Inherence factors are something the user and only the user is, such as fingerprints, voice, retina/iris patterns, and palmprints. Start with privileged, administrative, or remote-access users.

Resources for Taking Action

FTC Remote access guidance: *identifies tools to secure networks for employees and vendors who need remote access.*

NSA Defend Privileges and Accounts: *designed to limit exploitation and insider threat.*

Two Factor Auth (2FA): *lists websites that support multi-factor authentication.*

NSA Transition to Multi Factor Authentication: *outlines how to use Multi-factor Authentication to defend against an array of authentication attacks.*

NIST Digital Identity Guidelines

NIST Special Publication 1800-17: *Multifactor Authentication for E- Commerce*

Grant access and admin permissions based on need-to-know and least privilege. Restrict user access to only the information, networks, hardware and applications necessary. Are you asking why someone or something needs privileged access? Does the marketing team need access to the company's financial transactions? Does the reservations team need access to social media sites? Does a junior analyst need management-level admin/configuration privileges? Answering these questions helps you identify and implement need-to-know and least privilege to lower the risks of malware infections, data breaches, and insider threats.

Resources for Taking Action

NIST Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations: *this publication explains the principle of least prvillege and how to apply least priviliege to information systems.*

Center for Internet Security Benchmarks: *includes configuration guidelines for various technology groups to safeguard systems against today's evolving cyber threats.*

NSA Defend Privileges and Accounts: *designed to limit exploitation and insider threat.*

Develop IT policies/procedures to address changes in user status. Implement policies, processes, and technologies to ensure that only authorized users are granted the minimum privileges needed. Identify and deactivate unused accounts, eliminate shared accounts, remove unnecessary privileges and enforce strong password policies to dissuade cyber criminals from accessing your networks. Termination, separation, or even moves to other departments within the organization with different access requirements require attention to user access abilities.

Resources for Taking Action

NIST Cybersecurity Resource Center: *NIST's cybersecurity- and information security-related projects, publications, news, and events help support stakeholders.*

NIST Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publications Library: *includes guidelines, technical specifications, recommendations, and reference materials comprised of multiple sub-series.*

Cyber Readiness Institute Cyber Readiness Program: *contains information about reducing cyber risk and training materials for your employees.*

NIST Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security: *this publication provides security considerations for several remote access solutions.*

National Cyber Security Alliance Resources Library: *tips and resources to protect devices.*

SANS Security Policy Templates

Leverage unique passwords for all user accounts. Many cyber attacks occur due to weak and easy-to-guess passwords, so all passwords should be strong and unique, such as a sentence with numeric and non-numeric digits. Choose a pattern or template for your password that can be applied toward various accounts. This is something that is very individualized and therefore difficult to guess. A personal pattern or template allows for different passwords to be used for every account, while making it easy for the user and only the user to remember. Some hackers are more sophisticated and use algorithms to figure out passwords, so consider mechanisms that are stronger than password authentication such as biometrics, one-time passwords, and tokens for sensitive applications and functions.

Resources for Taking Action

Global Cyber Alliance Small Business Toolkit: *provides tips and actions to keep your accounts safer by moving beyond simple passwords.*

NIST Special Publication 800-63 Digital Identity Guidelines: *covers identity proofing and authentication of users interacting with government IT systems over open networks.*

CISA Creating and Managing Strong Passwords: *identifies six actions that users can take to create and manage strong passwords.*