ABOUT THIS GUIDE

Information about ransomware to help small and midsize businesses identify useful cybersecurity resources to meet their needs.

What Is Ransomware

And your small business

Making your business safer

About Our Company

McLeod Information Systems, LLC

is a comprehensive cybersecurity services company.

Our team has decades of experience servicing complex, multifaceted IT Security needs in warfare, private industry and government. Now we're bringing the best of breed practices to the marketplace.

Our mission it to provide our clients the peace of mind that their information is processed and protected in a secure infrastructure. We accomplish this by accessing process and procedures to implement security controls that mitigate risk.

Our services include:

- A & A Support
- Security Control Assessment (SCA)
- Vulnerbility Scan and Remediation
- Continuous Monitoring
- Policy Process and Development and Improvement
- Security Consulting

McLeod Information Systems

SDVOSB

1060 E. Montague Ave.
North Charleston, SC 29405
843.608.0582 ph
info@mcleidis.com
www.mcleodis.com

McLeod Information Systems

A SERVICE DISABLED VETERAN OWNED SMALL BUSINESS

Ransomware

A GUIDE FOR PREVENTION AND PROTECTION

SMALL AND MIDSIZE BUSINESSES

PREVENTION

- Implement an awareness and training progam. Employees should be made aware of the threat of ransomware and how it is delivered
- Patch operating systems, software, and firmware on devices. Patches help secure newly discovered security vulnerabilities in your system.
- Install anti-virus and anti-malware software. Also set them to automatically update and regulary scan.
- Manage the use of privileged accounts. No users should be assigned adminitrative access unless necessary then should be used only as needed.
- Configure access controls with least priviledges in mind.
- Disable macro scripts from office files transmitted via em-mail.

BUSINESS PROTECTION CONSIDERATIONS

- Back up data regularly, regularly verify the integrity of those backups.
- Back up data to an external hard drive.
- Secure your backups. Make sure the backups are not connected to the computers and networks they are backing up.
- Backups are critical in ransomware. If you are infected, this may be the best way to recover your critical data.

WHAT IS RANSOMWARE?

Ransomware is a malicous software that targets weaknesses in your computer systems. Once it has infiltrated your system, usually through phishing emails, it locks your system down and demands a ransom to be paid to reinstate access. Ransomware remains a popular means of attack, with new ransomware families being discovered every year. Prevention is the best way to protect yourself and your business from attacks.

THE RANSOM

The FBI does not support paying the ransom to the cybercriminals. Paying ransom does not guarantee an organization will regain access to their data. Paying ransom encourages the criminals to continue targeting other organizations for profit.

In all cases the FBI encouages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance. Victims are also encouraged to report cyber incidents to the FBI's Internet Crime Compliant Center (www.ic3.gov)

OTHER CONSIDERATIONS

- Use whitelisting software, which prevents unknown applications from executing.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and impliment physical/logical separation of networks and data for different organizational units.

To learn about additional resources beyond those recommended in this guide please contact McLeod IS.

www.mcleodis.com 843.608.0582