North Star
Small Business Data /Cyber Protection Awareness

AMERICA'S SBDC

RANSOMWARE

Ransomware is a form of malware that encrypts a victim's information and holds it for ransom. It is often designed to spread across a network and target all critical information, and can quickly paralyze an entire small business. It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for businesses and governmental organizations.

How Small Businesses Are Infected

Phishing
Clicking on links or opening attachments from attackers in emails.

Unsecure Websites
Visiting nonsecure, compromised websites can download malware.

Outdated Software
Old, unmaintained software may have vunerabilites attackers can leverage.

The Typical Attack Process

1. Cyber criminals gain admin access using above attacks
2. Your network is explored to locate and steal critical data
3. All backups and protections are destroyed
4. All data is encrypted and you are locked out
5. A ransom request is sent, with offer to unlock data
6. Cyber criminal receives ransom or data is published

How To Protect Your Small Business

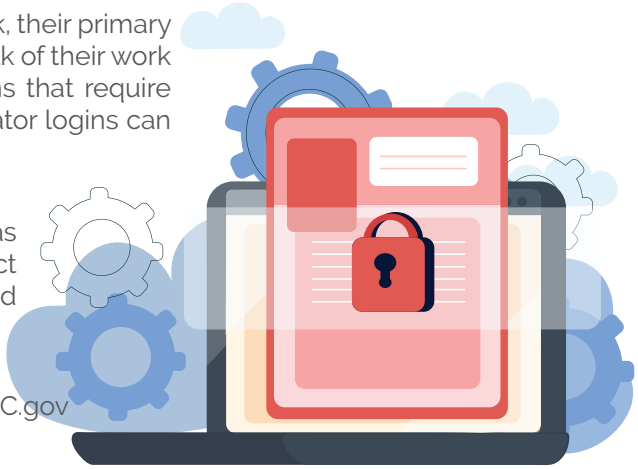
Backups - If your data has been encrypted and your backups are deleted, you are left with few choices. Paying the ransom and getting the key does not guarantee that your data remains intact and usable. Make your own encrypted backups daily. Consider how to isolate them to prevent deletion or destruction.

Patching & Updating - When a new update is released for software that patches a vulnerability, attackers immediately begin scanning the internet for vulnerable systems to exploit. While it may not be practical to patch instantly when an update is released, timely updates can reduce the chances of your system being compromised.

Network Segmentation - Nothing makes an attacker's job easier than a network where every system is accessible with one login, and there isn't any internal monitoring. Make sure you setup a network where only the systems that need to talk to each other are connected. Placing firewalls around critical data can help protect it from unwanted visitors.

Access Control - When an attacker gains access to your network, their primary goal is to gain administrative access to all systems. Typically the bulk of their work is performed in a semi-automated fashion using special programs that require administrative rights. Adding Multi Factor Authentication administrator logins can slow or stop their efforts.

Sensitive Data - Understanding what data you collect is just as important as protecting it. Determine if you actually need to collect all the data you have. Then make sure the data is encrypted and access to that data is tracked.



Resources: AmericasSBDC.org/Cybersecurity | StopRansomware.gov | FTC.gov