NorthStarInc

10 Best Practices to Help Prevent Ransomware Attacks

Ransomware is a type of malicious software that carries out the cryptoviral extortion attack from crypto virology that blocks access to data until a ransom is paid and displays a message requesting payment to unlock it. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse.

More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. The ransomware may also encrypt the computer's Master File Table (MFT) or the entire hard drive.

Here are 10 Best Practices to help prevent attacks:

1. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device. And backups should be stored offline. Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors/malicious scripts.)
2. Don’t open attachments in unsolicited emails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited email, even if the link seems benign. In cases of genuine URLs close out the emails and go to the organizations website directly through browser.
3. Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.
4. Configure access controls including file, directory, and network share permissions with least privilege in mind. If user only needs to read specific files, they should not have write access to those files, directories, or shares.
5. Maintain updated Antivirus software on all systems.
6. Block the attachments of file types: exe, pif, tmp, url, vb, vbe, scr, reg, cer, pst, cmd, com, bat, dll, dat, hlp, hta, js, wsf.
7. Keep the operating system third party applications (MS Office, browsers, browser plugins) up-to-date with the latest patches.
8. Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
9. Disable remote Desktop Connections, employ least-privileged accounts.
10. Enable personal firewalls on workstations.

Feel free to contact the team at North Star if you have questions about how to best prepare your business, and to implement any of the security tactics mentioned above**. Call 303-552-0018**.

NorthStarInc
Networks. Cloud. Security. Phones.