BankOnITUSA®

May 2017

8601 Commerce Park Drive, Oklahoma City, OK 73132 • Toll Free: 800-498-8877 • www.bankonitusa.com

Security Update

No Tears Here - BankOnIT's Got You Covered

The ransomware attack known as WannaCry, which has impacted more than 1 million worldwide, is an example of the evolution of typical ransomware attacks. Ransomware is malicious software that installs itself on a machine (the software could come from a malicious link, attachment, download, etc.) and then exploits a vulnerability to lock up files until the victim pays a ransom. Paying the ransom doesn't always guarantee the hacker(s) responsible will unlock the data.

BankOnIT's Threat Mitigation Shield is a multi-layered security approach developed exclusively by BankOnIT to help proactively protect against cyber threats. BankOnIT has confirmed that this includes protection from the WannaCry ransomware attack.

Following are a few of the security features BankOnIT has in place to help mitigate the threat of ransomware and other cyber attacks on your network:

- BankOnIT sits between your institution and the Internet at client institutions using BankOnIT's Managed Network (BMN) solution. This allows us to filter out a substantial amount of malicious traffic before it reaches your network.
- Web Content Filtering is utilized to help prevent connecting to malicious sites that contain cyber threats, such as ransomware.
- Outbound traffic is filtered to help limit the ability of a ransomware installation from connecting to servers on the Internet. These servers would authenticate the ransomware installation and lock up your files.
- The BankOnIT Management Agent (BMA) monitors the patch management system, helping keep machines up-to-date with the latest security updates, (including the patch for the WannaCry vulnerability).
- BankOnIT's Virtual Engineers monitor patches and update installations, providing a higher degree of successful deployments. The Virtual Engineers also alert human engineers on patch management and update challenges, allowing BankOnIT technical staff to review and address any update in question.
- BankOnIT performs quarterly Internal Vulnerability Assessments on your institution's network as a quality control check to help ensure that updates are being appropriately deployed.
- Real-time anti-virus protection is in place on workstations and servers throughout your institution's network.
- Backups are performed and available to help restore/recover data in the event of a ransomware event.
- Technical assistance with SAR filings for cybersecurity events as required.

Cybersecurity threats are constantly evolving and will continue to do so. For this reason, BankOnIT implemented its BankOnIT Threat Mitigation Shield to not only monitor for and alert on these threats, but to also block and resolve them when they do occur.

Your employees can help make your institution more secure as well by being aware that malware, such as ransomware, can be in a website, in an email, within an attachment or on a removable USB drive. Please remind employees to exercise caution when opening emails or attachments. If they are suspicious, they should not open the link, email or attachment.

BankOnIT is a CBSC preferred partner and provides cybersecurity e-newsletters for distribution to BankOnIT's clients' employees. BankOnIT clients, contact your Account Manager for previous articles or if you need another copy.

Bankers PRIVATE CLOUD®

Copyright © 2017 BankOnIT, L.L.C.

Disclaimer: This publication attempts to provide timely and accurate information concerning the subjects discussed. It is furnished with the understanding that it does not provide legal or other professional services. If legal or other expert assistance is required, the services of a qualified professional should be obtained.