Member FDIC
EQUAL HOUSING LENDER

First Bank & Trust Company
The Bank That Puts You First
Member FDIC

November 2017 Volume 3, Issue 11

Abingdon Virginia, East
276-628-3838
Abingdon Virginia, West
276-628-9558
Bridgewater Virginia
540-828-2020
Bristol Virginia, East
276-466-9222
Bristol Virginia, West
276-669-1122
Bristol Tennessee, Volunteer Pkwy
423-652-2022
Christiansburg Virginia
540-260-9060
Fairlawn Virginia
540-633-3793
Gray Tennessee
423-467-9966
Harrisonburg Virginia
540-434-0671
Johnson City Tennessee
423-975-9900
Kingsport Tennessee
423-246-3700
Lebanon Virginia, East
276-889-3401
Lebanon Virginia, West
276-889-4622
Lynchburg Virginia
434-455-0888
Norton Virginia
276-679-7401
Staunton Virginia
540-885-8000
Verona Virginia
540-248-7700
Waynesboro Virginia
540-943-5020
Wise Virginia
276-328-3439
Wytheville Virginia
276-228-1125

In this issue:

3 States of Data

For any organization, data is its biggest asset. Just as there are different types of data, there are also different states of data. Understanding the different states of digital data can help you select the kinds of security measures and encryption that are appropriate for protecting it.

1.

DATA AT REST

Data at rest is information that is not actively transmitting over networks. It is inactive data that is stored digitally and not being accessed on a regular basis. Data at rest is stored in different forms that includes, but is not limited to, offsite backups, data warehouses, hard drives or back up tapes. At this state, there can be additional layers of security added to it, such as encryption, multi-factor authentication, and both digital and physical access controls. Data at rest should almost always be encrypted to help avoid possible breaches.

2.

DATA IN MOTION

Data is at its most vulnerable state when it is in motion. Data in motion is data that is currently traveling across a network or on a computer ready to be read, updated, or processed. This can be data travelling over an untrusted or public network to a private, trusted network. The Internet will fall under the untrusted category while a corporate network will be categorized as private. Sending emails is one of the best examples of data in motion. When we send an email, it goes through an intricate process before it reaches the intended recipient. That process can sometimes be intercepted and fall into the hands of hackers. Data transmitting over any network whether local to cloud storage or from a central server to a remote terminal should be encrypted so that it cannot be hijacked by a hacker during any part of transmission from the original source to its final destination.

Continue on page 2

3.

DATA IN USE

Data in use is active data that is used every day. The data is readily available to the user and typically saved on computers. This type of data is also information that is accessed through multiple endpoints which makes it extremely vulnerable. The more devices that are accessing data the more room there is for a possible breach. Data in use is data that is not just being stored on a hard drive or external storage, it is also being processed by one or more applications. The data is currently in the process of being created, updated, added to, or erased. Data in use is susceptible to different kinds of threats depending on where it is in the system and who has access to it. Being able to track the who, what, when and where of data within an organization will help identify potential risk sooner rather than later. Although protecting data in use can sometimes be difficult because of the multiple ways the data can be accessed, having strong user authentication and strict profile permissions will help ensure that only individuals with the proper credentials are able to gain access to sensitive and confidential data.

Protecting data has been challenging in recent years and has highlighted the importance of the three states of data and understanding how each state plays a crucial part in an organization. The information provided in this write up are just some ways organizations can protect their data. Finding data security solutions that fit your organizations needs is essential to avoiding the unfortunate reality of data breaches that many organizations have faced. Organizations should work with their IT departments and security experts to determine risk factors and come up with a solid strategy that addresses any loopholes that can be a potential gateway for a cybercriminal.

Sources:
http://aspg.com/three-states-digital-data/#.We9E2rfrtbp
http://aspg.com/three-states-digital-data/#.We-WimiPLIU
https://www.datamotion.com/2015/12/best-practices-securing-data-at-rest-in-use-and-in-motion/

Good OnLine Habits!

Last month was National Security Awareness month, a month of concerted outreach from the industries best to both businesses and individuals. Each year, the campaign tries to raise awareness and educate us on the dangers that lurk on the Internet. Although this was just one month out of the year, the other 334 days should be treated with the same importance in terms of cybersecurity.

One of the major campaigns featured during National Security Awareness month is The STOP. THINK. CONNECT campaign. The campaign is used to reach a global audience to promote a more secure online environment. The STOP. THINK. CONNECT campaign not only educates, but it also provides great resources. One of last month's highlights promoted by the campaign was best practices to help encourage safe online habits. Some of these habits are listed below and should be used daily and shared with everyone we know!

Keep a clean machine

- Make sure all software is current
- Protect all devices that connect to the Internet, including Xbox units, PlayStation devices, iPads and any other electronic entertainment gadgets.

Protect your personal information

- Create strong passwords. It's been said over and over again, but it is worth repeating. Create passwords that are unique and have at least twelve characters.

Connect with care

- Be mindful of the links you receive in your emails, social media posts and in other advertisements. If something seems suspicious, don't second guess yourself, just delete it!
- Don't conduct important businesses transactions, such as banking, on public Wi-Fi networks.
- When shopping online, make sure the website you are using is security-enabled by looking for https:// or shttp://.

Be Web-Wise

- It can seem like we are all in a state of information overload, but it is important to keep up with the latest and most reliable ways to stay safe online.
- Protect your valuable information by creating backups.

Be a good online citizen

- Practicing good online behavior can have a far greater impact than you think.
- Be cognizant about what you post online.
- Help authorities catch cybercriminals by reporting suspicious activity.

To learn more and to get more great tips and advice that can be shared with family and friends visit

https://www.stopthinkconnect.org/.