MARCH 2019
ISSUE 3

First Bank & Trust Company

The Bank That Puts You First

Member FDIC

Inside This Issue

Six Security Problems You Might Not Realize You Have

Every organization has a lot to contend with every day. The external and internal day-to-day transactions of a business can sometimes cause distractions. In an age where security threats are at its highest, we can tend to look for the obvious; however, sometimes there are more subtle — but equally destructive — risks that fall through the cracks.

IT administrators are tasked with a lot and are often extremely busy just trying to keep up with their daily functions. Below are six security risks you may not be aware of.

1. Your Employees

No organization can reach its full potential without the help of their employees. However, sometimes employees are the biggest source of security risks. Employees have the most access to a company's data. We expend a lot of effort worrying about external threats, but in all honesty, all it takes is an employee to click on a link via phishing email. Sometimes a well-meaning employee can make a major mistake. Good governance, education and setting (and enforcing) policies are your best steps to closing the holes.

2. Unauthorized Machines

Bring Your Own Device (BYOD) is the newest trend but it also comes with risks. If an employee decides to circumvent the network to do something your existing infrastructure doesn't allow them to do, it could lead to a huge security risk. Knowing what is connected to a network at all times is a good way to stay protected.

3. Ancient Servers

There is always that one server that is hanging on for dear life. It's usually the one running a software package that is impossible to migrate to another machine. But all hardware reaches end-of-life at some point. Holding onto equipment longer than we should is not ideal. Technology is moving at an extremely fast rate. Manufactures are constantly improving old technology and one major benefit to that is security gets more robust. Old hardware may not get the necessary updates or patches required and it may not be compatible with the newest software. The life of a server is typically five years. If your organization is operating on anything over that, it may be time to consider replacing it.

EQUAL HOUSING LENDER

Member FDIC

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

Operations Center
276-623-2265

5. Local Admins

We all know the dangers of allowing users to run with escalated privileges. Still, we occasionally end up with users being granted local admin rights inappropriately. It is imperative that the appropriate people have appropriate access within an organization. These guidelines will help ensure the organization and its customers' data is secure.

6. Incorrect Share/File Permissions

File sharing is a way for collaborative user files that are too large to send as email attachments to be easily accessed. However, file sharing is also a highly vulnerable practice, and if done incorrectly, can put corporate data at risk. To avoid mishaps, your organization should establish a share and file structure with appropriate permissions.

Sources:
https://www.techrepublic.com/blog/10-things/10-security-problems-you-might-not-realize-you-have/https://www.forbes.com/sites/tonybradley/2018/01/27/top-5-concerns-to-focus-on-for-data-privacy-day/

How to Dispose of Your Devices Safely and Securely

Mobile devices, such as smartphones, smartwatches, and tablets are our lifeline. Some of us are literally lost without them. These devices store far more sensitive data than you may realize, oftentimes more than even your computer. They continue to advance and innovate at an astonishing rate and as a result, some people replace their mobile devices as often as every year. But once the old device has been replaced with the latest and greatest model, what do you do with the old one? Unfortunately, too many people don't take the time to think this part through and dispose of their devices with little thought on just how much personal data is on them.

Regardless of how you dispose of your mobile device, such as donating it, exchanging it for a new one, giving it to another family member, reselling it, or even throwing it out, you need to be sure you first erase all of that sensitive information. You may not realize it, but simply deleting data is not enough; it can easily be recovered using free tools found on the Internet. Instead, you need to securely erase all the data on your device, which is called wiping. This actually overwrites the information, ensuring it cannot be recovered or rendering it unrecoverable. Remember, before you wipe all of your data, be sure to back it up first. This way, you can easily rebuild your new device.

The easiest way to securely wipe your device is to use its "factory reset" function. This will return the device to the condition it was in when you first bought it. The factory reset will provide the most secure and simplest method for removing data from your mobile device. But note: the factory reset function varies among devices.

Sources:
https://datafloq.com/read/5-Security-Vulnerabilities-Looming-Internet-Things/2127
https://www.iworkbarcoda.com/article/top-10-cve-vulnerabilities-of-2018/4134.13

In addition to the data stored on your device, you also need to consider what to do with your SIM (Subscriber Identity Module) card. A SIM card is what a mobile device uses to make a cellular or data connection. When you perform a factory reset on your device, the SIM card retains information about your account that is tied to you, the user. If you are keeping your phone number and moving to a new device, talk to your phone service provider about transferring your SIM card. If this is not possible (for example, if your new phone uses a different size SIM card), keep your old SIM card and physically shred or destroy it to prevent someone else from reusing it.

"Unfortunately, too many people don't take the time to think this part through and dispose of their devices with little thought on just how much personal data is on them."

Also, some mobile devices utilize a separate SD (Secure Digital) card for additional storage. These storage cards often contain pictures, smartphone applications, and other sensitive content. Remember to remove any external storage cards from your mobile device prior to disposal. (For some devices, your SD cards may be hidden in the battery compartment of your device, possibly beneath the battery). These cards can often be reused in new mobile devices, or can be used as generic storage on your computer with a USB adapter. If reusing your SD card is not possible, then just like your old SIM card, we recommend you physically destroy it.

If you are unsure of how to make the transition to a new device securely, you can always seek the assistance from your mobile device carrier or the manufacture and get help from a trained technician. Finally, before throwing the device away and after safely and securely wiping it, think of other useful options for it, like donating it to a charitable organization, recycling it or even passing it on to a friend or family member.

Sources:
https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device
https://www.techrepublic.com/article/10-places-to-recycle-your-cell-phone/