UNION BANK

NOVEMBER 2019 Issue 11

Mobile Banking App is HERE!

THE 3 STATES OF DATA

AND HOW TO PROTECT IT

Member FDIC

EQUAL HOUSING LENDER

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.

Data at Rest

Data at rest is inactive data that is stored digitally and is not actively transmitting over networks or being accessed on a regular basis. Data at rest is stored in different forms that include, but is not limited to, offsite backups, data warehouses, hard drives or backup 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 protection helps companies or other controlling parties ensure that stored data is not vulnerable to hacking or other unauthorized access. Data at rest should almost always be encrypted to help avoid possible breaches.

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

Continued on page 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. Data in motion is very susceptible to human error, network failures and insecure file sharing. Some ways to help protect data in motion is to restrict certain types of cloud based sharing. Cloud-based apps, such as Dropbox and Google Drive, oftentimes do not meet company standards for data protection and encryption and can sometimes allow IT teams from protecting the company's data. Also make sure that encryptions are appropriately set with permissions to ensure only authorized users can access certain files. That way in the event a file with sensitive data gets emailed to somebody in error, they are unable to open the file. In addition, be sure to monitor where shared files are going. If a file is sent to an unauthorized recipient, IT can get notified and recall the document immediately.

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, data in transit should be an essential part of organization's data protection strategy. 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 organization's 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:
https://www.google.com/search?q=protect+data+in+use&ei=DhazXcuuAq_t5gKMwZ24CA&start=10&sa=N&ved=0ahUKEwjL7Z6a3rfAhWvtlkKHYxgB4cQ8tMDCNw8&biw=1366&bih=651
http://espg.com/three-states-digital-data/#.We9E2rItbp
http://espg.com/three-states-digital-data/#.We-WimPLIU
https://www.datamotion.com/2015/12/best-practices-securing-data-at-rest-in-use-and-in-motion/

THE IMPORTANCE OF DEVICE UPDATES

You've most likely heard the word "patches" several times when discussing IT, and with good reason. Patches are one of the most important cybersecurity tools to help protect against malware and viruses. But did you know that patches not only apply to workstations but also to mobile devices as well?

For most users, patches and updates are probably one of the most annoying parts of using your devices. Just when you are about to score those points on your favorite mobile app game, the updates force you to unexpectedly stop whatever you're doing and wait until your software is up to date. Despite being a temporary nuisance, software updates and hardware upgrades are vital and necessary. Our digital world is plagued with exploits and vulnerabilities and the need to make sure devices are up to date with the most current software and upgrades are simply part of living in a digital time.

Hackers are continuously looking for the next loophole so they can exploit a vulnerability and companies who create the devices are constantly coming up with ways to close exposed loopholes or prevent new ones from occurring. To do that, updates are needed to help prevent devices from being hijacked by hackers.

We use our mobile devices in some cases more than we use our laptops or desktops, especially for banking transactions. Smart phones have made banking seamless, from transferring funds within seconds to making purchases with just a scan of a barcode on your phone. Because of that, mobile devices should be just as secure as those other devices, if not more so.

The software updates also improve the performance of your device, sometimes updating graphics and enhancing the usability of the device.

Software updates should be done as soon as they are available. It is an important step in keeping your device up to date with the latest and greatest tools and protecting your data!

Sources:
https://blog.pradeo.com/why-mobile-os-application-updates-are-so-important
https://www.fcc.gov/consumers/guides/updating-your-smartphone-operating-system