**IOT & Cyber Security**

~Week 1-2~

End of Unit Activities

**Activity 1**

***Cloud platforms are becoming a very common commodity in the digital system. What are the benefits and draw backs in Cloud solutions with respect to cyber security? Present an argument with minimum 500 words in favour of or against cloud storage. What are the security risks involved in cloud vs local store . You should post your solution in the discussion group and provide at least two references.***

There are several benefits and drawbacks to using cloud storage solutions for cyber security.

**Benefits:**

1. **Scalability:** One of the main benefits of using cloud storage is the ability to scale up or down as needed. This is particularly useful for businesses that experience fluctuating storage needs, as they can easily adjust their storage capacity to meet their current requirements.
2. **Cost-effectiveness:** Cloud storage is often more cost effective than traditional on-premises storage solutions. This is because businesses only pay for the storage they actually use, rather than having to invest in physical hardware and infrastructure.
3. **Automatic updates:** Cloud storage providers regularly update their systems to improve performance and security. This means that businesses using cloud storage don't have to worry about manually updating their systems or installing patches.
4. **Data backup and recovery:** Cloud storage providers often offer data backup and recovery services as part of their packages. This means that businesses can have peace of mind knowing that their data is being regularly backed up and can be recovered in the event of a disaster.

**Accessibility:** Cloud storage allows users to access their data from anywhere with an internet connection. This is particularly useful for businesses that have employees working remotely or on the go.

**Drawbacks:**

1. **Dependence on internet connection:** In order to access cloud storage, users must have an internet connection. This can be a problem in areas with unreliable or non-existent internet access.
2. **Security concerns:** One of the main drawbacks of using cloud storage is the potential for security breaches. While cloud storage providers have measures in place to protect data, there is still a risk that data could be accessed by unauthorized parties.
3. **Control:** When data is stored in the cloud, businesses must rely on the cloud storage provider to maintain and secure their data. This can be a concern for businesses that prefer to have more control over their data.
4. **Limited customization:** Cloud storage providers often have limited customization options, which can be a problem for businesses with specific storage needs.
5. **Vendor lock-in:** Businesses that use cloud storage may become reliant on a particular provider, which can be problematic if the provider experiences problems or the business wants to switch to a different provider.
6. In terms of security risks, there are a few key differences between cloud storage and local storage. One of the main risks with cloud storage is the potential for data breaches. While cloud storage providers have measures in place to prevent data breaches, there is still a risk that data could be accessed by unauthorized parties.
7. On the other hand, local storage has the risk of physical damage or theft. If a device with local storage is lost or stolen, the data on it could be accessed by unauthorized parties. Additionally, local storage is vulnerable to damage from natural disasters such as fires or floods.
8. Overall, the decision to use cloud storage or local storage will depend on the specific needs and risks of a business. It is important for businesses to carefully consider the benefits and drawbacks of each option and choose the one that best meets their needs.

**References:**

* Cloud Storage: Benefits, Risks, and Best Practices. (n.d.). Retrieved from <https://www.verizon.com/about/our-company/verizon-risk-report/cloud-storage-benefits-risks-best-practices/>
* Cloud vs. On-Premises Storage: Which is Right for Your Business? (2018, August 7). Retrieved from <https://www.cio.com/article/3296429/cloud-vs-on-premises-storage-which-is-right-for-your>

**Activity 2**

***A-) In 2017 a ransomware termed as WannaCry unleased its malicious attack on a global scale. What cautions and safeguards should have been in place that could have averted this attack?***

The WannaCry ransomware attack in 2017 was a global cyber attack that affected more than 200,000 computers in 150 countries. It exploited a vulnerability in older versions of the Windows operating system and encrypted users' data, demanding payment in order to decrypt the data.

**WannaCry attack:** Keep software and operating systems up to date: One of the main reasons the WannaCry attack was so successful was that it exploited a vulnerability in older versions of the Windows operating system. Ensuring that all software and operating systems are kept up to date with the latest patches and security updates can help prevent similar attacks from being successful.

**Use antivirus software:** Antivirus software can help protect against malware such as ransomware by detecting and blocking malicious files. It is important to keep antivirus software up to date to ensure it can detect the latest threats.

**Implement a firewall:** A firewall can help protect against cyber attacks by blocking unauthorized access to a network. It is important to configure the firewall properly to ensure it is effective at blocking unwanted traffic.

**Use strong passwords:** Using strong, unique passwords can help prevent unauthorized access to accounts and systems. It is also important to use different passwords for different accounts and to change them regularly.

**Regularly back up data:** Regularly backing up data can help mitigate the impact of a ransomware attack. If data is backed up, it can be restored if it is encrypted by ransomware.

**Educate employees:** Ensuring that employees are aware of cyber security best practices, such as avoiding clicking on links in suspicious emails and not sharing passwords, can help prevent successful attacks.

**Use multi-factor authentication:** Implementing multi-factor authentication can add an extra layer of security to accounts and systems. With multi-factor authentication, a user must provide an additional piece of information, such as a code sent to their phone, in order to access an account.

By implementing these precautions and safeguards, businesses can help protect themselves against cyber attacks such as the WannaCry ransomware attack.

**References:**

WannaCry ransomware: What you need to know. (2017, May 15). Retrieved from <https://www.csoonline.com/article/3194747/wannacry-ransomware-what-you-need-to-know.html>

WannaCry ransomware attack: What you need to know. (2017, May 15). Retrieved from <https://www.theverge.com/2017/5/15/15634764/wannacry-ransomware-cyber-attack-what-you-need-to-know>

***B-) List the security measures you would take to safeguard your computer against attacks that are caused by legacy software without updates. Consider both scenarios where there is an option for a software update and without it. Write at least 100 words for each case.***

Here are some security measures that can be taken to safeguard a computer against attacks caused by legacy software:

* Install a firewall and keep it up to date to block unauthorized incoming and outgoing traffic.
* Install and regularly update antivirus software to detect and remove malware.
* Enable automatic updates for the operating system and other software to ensure that the latest security patches are installed.
* Use a web browser with built-in security features, such as Google Chrome, which blocks malicious websites and downloads.
* Enable two-factor authentication for online accounts to add an extra layer of protection.
* Avoid clicking on links in emails or online that seem suspicious or too good to be true.
* Create strong and unique passwords for all online accounts and use a password manager to store them securely.
* Avoid using public Wi-Fi networks, as they can be vulnerable to attacks.
* Regularly back up important data to a separate location to prevent data loss in case of an attack.
* Consider using a virtual private network (VPN) to encrypt internet traffic and protect against snooping.
* If the legacy software does not have an option for an update:
* Isolate the legacy software by running it on a separate device or in a virtual environment.
* Use a sandbox to test any potentially dangerous files before opening them on the main device.
* Consider replacing the legacy software with a newer version that receives regular updates.
* Regularly monitor the device and the legacy software for any unusual activity or vulnerabilities.
* Consider hiring a security professional to assess the risks and provide additional security measures.

**Activity 3**

***Why is it important to have a backup system in place that works closely with cyber security framework? How are these two components are related? Please use your own personal computer as hypothetical machine and list the steps that you will adopt to backup your data.***

It is important to have a backup system in place that works closely with the cyber security framework because a backup system can help protect against data loss due to cyber attacks, hardware failures, or other types of disasters. For example, if a computer is infected with malware that corrupts or deletes important files, a recent backup can be used to restore the lost data.

To create a backup system for a personal computer, the following steps can be taken:

1. Identify the data that needs to be backed up. This might include documents, photos, music, and other types of files.
2. Choose a backup method. Options might include an external hard drive, cloud storage, or a physical media such as a USB drive or DVD.
3. Set up a schedule for backups. It is important to create regular backups to ensure that the most recent version of the data is always available.
4. Test the backup system to ensure that it is working properly and that the data can be successfully restored.
5. Store the backup in a secure location, such as a locked cabinet or safe deposit box, to prevent unauthorized access or physical damage.
6. By following these steps, it is possible to create a backup system that works closely with the cyber security framework to protect against data loss and other types of disasters.

17330118 – Mustafa Guner Guner