BITS 3523 COMPUTER AUDIT & RISK MANAGEMENT
LAB 5 (EXERCISE)

Computer Audit

NAME: FATIN NASUHA BINTI MOHAMED SABIR
MATRIC NO: B032110289
PROGRAMME: 3 BITZ S1G1

Instructions:
1. Solve the below given question and submit the softcopy which may contain your answers via the ULearn portal.

Questions [1]

You are required to identify **FIVE** significant elements related to computer security in your PC/Laptop. Conduct auditing process against your chosen elements. An example of auditing process are as follows:

Antivirus

1. *Name*
2. *Install date*
3. *Last update date*
4. *Able to identify unknown malware?*
5. *Total signature 6. Etc.*

You must provide your suggestion or recommendation if chosen elements need significant configuration changes or updates as well as give cause why such changes/updates needed.

Antivirus

1. **Name**: Microsoft Defender Antivirus
2. **Install date**: 7/5/2022
3. **Last update date**: 15/4/2024
4. **Able to identify unknown malware?**
   Yes. This is because Microsoft Defender Antivirus uses the "block at first sight" method to detect new malware and block it within seconds. When the antivirus encounters a suspicious but undetected file, it queries the Microsoft cloud protection backend. This cloud backend applies heuristics, machine learning and automated analysis of the file to determine whether the files are malicious or not.
5. **Total signature:**
   Microsoft Defender Antivirus stopped using static signature-based engine in 2015. Instead it utilizes a model that uses predictive technologies such as machine learning, applied science and artificial intelligence to protect the device from evolving malwares.
6. **Recommendation**: Perform regular scans to remove potentially harmful files or malware that may have evaded real-time protection.

Device Encryption

1. **Configuration Status:** Enabled
2. **Name:** BitLocker Drive Encryption
3. **Related Drives:** Operating system drive (OS (C:) and Fixed data drive (New Volume (D:))
4. **Is the recovery key already backed up?**
   Yes. The recovery key has been backed up on several places.
5. **For fixed data drives, is the password has been set?**
   No
6. **Recommendation:** Set a password for the fixed data drive (D:) to ensure that it cannot be accessed without the password if the drive is removed from the device.

Firewall

1. **Firewall status**
   a. Domain network: On
   b. Private network: On
   c. Public network: On
2. **Name:** Windows Defender Firewall
3. **Updates:** Managed by Windows Security
4. **Firewall rule:** Default
5. **Default outbound rule:** Outbound connections that do not match a rule are allowed.
6. **Connection security rules:** Default
7. **Recommendation:** Keep the firewall on to receive Windows Security Updates automatically.

Operating System Updates

1. **Name:** Windows Update
2. **Last Update date:** 19/4/2024
3. **Pending update:** No pending updates
4. **Recommendation:** Enable automatic updates to receive security patches as soon as it is available

Password Management

1. **Name: Windows Hello**
2. **Sign-in method: There are three sign option offered which are Facial recognition, fingerprint recognition, and PIN**
3. **PIN complexity:** The PIN are not limited to numbers only. There are options to include letters and symbol for the PIN.
4. **Recommendation:** Enable multi-factor authentication (MFA) to add extra layer of security.

-END-