|  |
| --- |
| COSC130 |
| Small business cybersecurity plan. |
| Assignment 3 |

|  |
| --- |
| Ben Murarotto  8-9-2024 |

**Step 1 – Securing the network.**

1. Purchase and configure firewall/network switch – Assuming the service will have low to medium traffic but involve high sensitivity information we will want to ensure our firewall can take advantage of advanced security settings for packet filtering. We also want to dedicate the greatest portion of the budget here as protecting our systems is the highest priority for a small business. The Cisco Meraki MX68 retails at roughly $780 AUD and supports our current needs with room for potential upscaling. We want to utilise its features such as packet inspection, intrusion detection/prevention and advanced malware protection. We also want to restrict all ports not required by our web services. This should give us sufficient protection against direct attacks to our business network. We also may want to consider the firewall’s geolocation feature to restrict traffic from regions we don’t expect legitimate buyers from.
2. Employ a web application firewall (WAF) – Since our company’s service will be entirely browser based, we will want to utilise a WAF to protect the site directly from malicious activity. This will keep our services safe and accessible by employing DDoS mitigation systems, protect databases from attacks like SQL injection and filtering and denying unwanted traffic from suspicious users and bots. Since the team is inexperienced the cloud based WAF option is highly desirable. By using a cloud-based service from a reliable provider like Amazon Web Services, we can take a hands-off approach in this area and allow them to handle updates and maintenance. It is also the best approach for future business scaling and will allow the team to prioritise efforts elsewhere.
3. Finally, we will establish access control to ensure only trusted individuals (and myself) can manipulate network settings.

**Step 2 – Setting up local devices.**

1. The first step will be to update the PC’s firmware, OS, and application software.
2. Next we will want to set-up a low cost antivirus for each system to protect from malware and virus threats. Norton Antivirus can protect all our devices for less than $55 per year and is a reliable choice in this case. It provides all kinds of threat detection as well as backup for compromised systems.
3. The next step is to implement a password manager to supplement the office and trading tools on each system. Bitwarden is a cheap and effective password management system costing roughly $100 per year for each device.
4. Since the company has no dedicated server and we don’t necessarily want to pay for cloud services if we don’t have to, we will assume that one of the local machines will be hosting the website and database queries. On the dedicated host machine, we will ensure encryption exists in the database file to protect the sensitive user data. We also will be using Windows free disk encryption software called BitLocker to physically encrypt the disk of all local machine devices.

**Step 3 – Training and response protocol.**

1. Phishing awareness – Teach the team about phishing scams and common methods (email, phone, text). Emphasise the importance of ensuring who is communicating with us and the kinds of information they are after, typically sincere sources will not enquire about sensitive data through these channels.
2. Malware awareness – Teach the team how to keep software and firmware up to date and the dangers of downloading unrecognisable files. We can also utilise router settings and antivirus settings to avoid dangerous files and websites all together.
3. Discuss social engineering concepts – Teach the team about how some malicious actors may try coax or bait you into exposing sensitive information – provide scenarios about how scammers have posed as IT consultants in the past to try and gain access to desktops.
4. Provide safe internet usage guidelines – Include information about email and communication practices, discuss sensitive information only through secure channels. Ensure you aren’t utilising work systems for non-work related activity etc.
5. Create a response protocol - In case of a security incident, we will have a well-defined incident response protocol to minimise harm and ensure a swift recovery. Team members should immediately report any suspicious activity or potential security breaches to myself. Communication with affected stakeholders, including customers, banks, and regulatory bodies, should be timely and transparent to maintain trust. Annual training will be done to ensure all employees are familiar with these procedures and can act quickly when necessary.