|  |  |
| --- | --- |
| **Unit Code:** | ENSN201 |
| **Type of Assessment:** | Formative Assessment |
| **Length/Duration:** | One page of answer |

**Week 6**

**Questions:**

Read the news below on Cyber Attack on Optus Network.

<https://7news.com.au/news/optus-slammed-after-massive-cyber-attack-an-email-is-not-going-to-cut-it-c-8420317>

Now answer the following questions:

1. Explain the impact of this cyber attack on the Optus Customers.

Ans:

**Impact of the Cyber Attack on Optus Customers:**

The Optus cyber-attack, one of the largest data breaches in Australian history, had profound and multifaceted consequences for millions of customers. The breach exposed sensitive personal information of up to 9.8 million current and former Optus users, including names, dates of birth, phone numbers, email and home addresses, and critical government-issued identification documents such as driver’s license numbers, passport details, and Medicare numbers. For approximately 10,000 customers, this data was publicly released on the dark web, significantly elevating their risk of identity theft, financial fraud, and targeted scams. The exposure of government ID numbers forced affected individuals to undergo the cumbersome process of replacing documents like driver’s licenses and passports, with state agencies like the Department of Transport and Main Roads in Queensland replacing over 178,000 licenses alone.

The breach also eroded trust in Optus due to its delayed and inadequate response. Customers criticized the company for failing to promptly notify them about the extent of the compromise, with many learning about the exposure of their Medicare numbers days after the initial announcement. The Australian government publicly rebuked Optus for relying on email notifications, which were deemed insufficient for communicating the severity of the incident. This lack of transparency left customers uncertain about how to protect themselves, exacerbating anxiety and frustration.

Financial risks became a immediate concern, as cybercriminals could use stolen data to open fraudulent accounts, apply for loans, or make unauthorized purchases. The hacker’s $1.5 million ransom demand and subsequent release of data highlighted the persistent threat of further exploitation. Even after the threat actor claimed to delete the data, experts warned that the information could resurface on criminal marketplaces, subjecting victims to long-term vulnerabilities.

The breach also triggered legal and institutional repercussions. A class-action lawsuit was filed against Optus, alleging negligence in safeguarding customer data. The incident prompted scrutiny of Australia’s privacy laws, with calls for stricter regulations akin to the EU’s GDPR. Optus faced reputational damage, estimated to have lost $1.5 billion in brand value, and incurred significant costs for remediation, credit monitoring services, and potential compensation.

Emotionally, customers experienced heightened stress and distrust, knowing their personal information could be misused indefinitely. The breach underscored the fragility of digital security and left many questioning the adequacy of corporate accountability in protecting consumer data. For Optus, the attack highlighted systemic failures, including unsecured APIs and lax security protocols, which allowed hackers to exploit vulnerabilities undetected for months. The aftermath of the breach continues to affect customers, serving as a stark reminder of the enduring consequences of large-scale data compromises.

1. What is your suggestion for us to keep us safe from cyber-attack.

Ans:

**Suggestions to Stay Safe from Cyber Attacks**

**Implement Strong Password Practices:**

Create unique, complex passwords for every account, avoiding predictable details like birthdays or names. Use a reputable password manager to generate and store passwords securely. Never reuse passwords across multiple platforms, as this increases vulnerability if one account is compromised.

**Enable Multi-Factor Authentication (MFA):**

Activate MFA on all accounts that offer it. Use verification methods such as fingerprint scans, one-time codes from authentication apps, or hardware security keys. This adds a critical layer of protection even if your password is stolen.

**Regularly Update Software and Systems:**

Install updates for operating systems, applications, and antivirus programs immediately. Enable automatic updates to ensure continuous protection against newly discovered vulnerabilities. Outdated software is a prime target for hackers.

**Use Anti-Virus and Firewall Protection:**

Install reputable anti-virus and anti-malware tools to detect and block malicious software. Pair these with a firewall to monitor network traffic and block unauthorized access attempts. Regularly scan devices for threats.

**Exercise Caution with Emails and Links:**

Verify the sender’s identity before opening attachments or clicking links, especially in unsolicited messages. Avoid responding to urgent requests for personal or financial information, which are often phishing attempts.

**Secure Wi-Fi Networks:**

Protect home Wi-Fi with a strong password and WPA3 encryption. Avoid conducting sensitive transactions on public Wi-Fi; if necessary, use a VPN to encrypt data. Set up a separate guest network for visitors.

**Back Up Critical Data:**

Regularly back up important files to external drives or encrypted cloud storage. This minimizes disruption from ransomware attacks or hardware failures, allowing you to restore data without paying ransoms.

**Monitor Financial and Online Accounts:**

Check bank statements, credit reports, and online accounts frequently for unauthorized activity. Set up real-time alerts for transactions to detect fraud early. Report suspicious activity immediately.

**Limit Personal Information Sharing:**

Reduce the amount of personal data shared on social media and other platforms. Adjust privacy settings to restrict access to your information. Only provide necessary details when creating online accounts.

**Stay Informed About Cyber Threats:**

Follow trusted cybersecurity sources to learn about emerging threats like social engineering. Participate in training sessions to recognize and avoid evolving scams.

**Secure Mobile Devices:**

Enable biometric authentication (e.g., fingerprint or facial recognition) on smartphones. Disable Bluetooth and location services when not in use. Download apps only from official stores to avoid malware.

**Marking Guide (Rubric):**

**Total Marks: 20**

|  |  |  |  |
| --- | --- | --- | --- |
| **Marking Criteria** | **Lecturer Expectation** | **Marks** | **Comments** |
| Analysis | Questions answered and covered in Depth |  |  |
| Concept | Demonstrates good understanding of key concepts |  |  |
| Idea | Original and creative thoughts |  |  |
| Critical Analysis | Critical and evaluative analysis of relative importance of issues |  |  |