Assignment #1

What was Taken?

Background / Scenario

Security breaches occur when individuals or applications are trying to gain unauthorized access to data, applications, services, or devices. During these breaches, the attackers, whether they are insiders or not, attempt to obtain information that they could use for financial gains or other advantages. In this assignment, you will explore a few security breaches to determine what was taken, what exploits were used, and what you can do to protect yourself.

Security Breach Research

Incident Date	Affected Organization	How many victims? What was Taken?	What exploits were used? How do you protect yourself?	Reference Source (Hyperlink)
August 24, 2024.	**GMA Network**, a major television network in the Philippines.	● The hackers accessed and exposed **outdated project files** related to various GMA Network projects, such as "BATANGAS 2023," "BATANGAS 2024," and "CEBU MASTERCLASS." No sensitive or personal information was compromised.	- The hackers exploited a **known vulnerability in IBM Aspera**, a third-party file transfer system used by GMA Network. This vulnerability had not been patched, leaving the network exposed. - To protect us from this kind of breach, we must keep our software updated, use strong passwords, be cautious of phishing, enable two-factor authentication, and back up your data.	Deep Web Konek
May 2023	**TESLA**	● Personal information of employees and production secrets leaked. ● The breach led to the exposure of the personal data of 75,000 people, which could potentially result in a $3.3 billion GDPR fine	- Insufficient protection of sensitive personal data - The details on how the perpetrators obtained access to the sensitive data are not publicly available. - Proper onboarding and	Ekran Case#5

			termination procedures - Conducting a user access review - Monitoring user activity	
Late September 2023 (Initial breach detected)	**Okta,** a leading identity and authentication platform	● While the exact number is difficult to ascertain, the breach impacted nearly all Okta customer support users, potentially affecting thousands of organizations. ● The attackers stole the names and email addresses of nearly all Okta customer support system users. For a smaller subset, additional data like last login, username, phone number, and company name was also compromised.	- The attackers exploited a compromised service account belonging to an Okta employee. This account was used to gain unauthorized access to the customer support system. - **Use MFA:** Enable MFA for all privileged accounts. **Strong passwords:** Change passwords regularly and avoid using easily guessable information. **Beware of phishing:** Be cautious of suspicious emails. **Limit access:** Restrict access to sensitive systems and data. **Monitor for unusual activity:** Keep an eye out for unusual login attempts or changes to your accounts.	KrebsOnSecurity
Throughout 2022	**T-Mobile**	● The exact number of victims is unknown, but it could be significant. ● SIM control of targeted mobile phone numbers ● Potential access to financial, email, and social media accounts linked to those phone numbers	- Phishing attacks targeting T-Mobile employees - Social engineering tactics to trick employees into giving up login credentials - Enable strong multi-factor authentication (MFA) that does not	KrebsOnSecurity

			rely on SMS messages, such as security keys. - Be wary of phishing attempts. -Do not click on suspicious links or enter your credentials on unknown websites. - Consider using a separate phone number for your most sensitive accounts.	
Between January 18 and February 24.	**ARcare, a US healthcare provider**	- Approximately 345,353 individuals are victims of this breach - Sensitive medical and personal data, including names, Social Security numbers, driver's license information, financial account information, medical treatment information, and health insurance information.	- The specific exploits used are not publicly disclosed, but the breach likely involved unauthorized access to ARcare's computer systems. - **Monitor accounts:** Regularly review account statements and credit reports for suspicious activity. **Report suspicious activity:** Contact your healthcare provider, insurance company, or financial institution if you notice anything unusual. **Protect personal information:** Be cautious about sharing personal data online and avoid clicking on suspicious links.	PortSwigger

Prepared By:

JAYSON ASIADO - BSCS3A