**Case Study Analysis: Capital One Data Breach**

Name of Case and Link: Capital One Data Breach (https://www.upguard.com/blog/biggest-data-breaches-us)Date of Case: July 2019Why Did This Case Make the News? The Capital One data breach was a major incident because it exposed personal information of over 100 million customers. The breach occurred due to a misconfigured web application firewall (WAF), which allowed unauthorized access to sensitive data. This event highlighted the growing risks of cloud security vulnerabilities and raised concerns about how financial institutions protect personal and financial information. It also demonstrated how a single misconfiguration could lead to large-scale security failures, affecting millions of customers.

Describe the Breach Type of Security or Data Breach: The breach involved unauthorized access to customer data due to a misconfigured WAF. The exposed information included Social Security numbers, bank account details, and credit scores. Why Was This Company a Target? Capital One, as a large financial institution, stored vast amounts of personally identifiable information (PII). Cybercriminals target such organizations because of the high value of financial and personal data, which can be used for identity theft, fraud, and black-market sales. In this case, the attacker exploited a weakness in the cloud security setup to gain access.

Identify the Threat(s)Immediate Threat(s): The exposure of sensitive customer data created a high risk of identity theft and financial fraud. Criminals could use the stolen information to access bank accounts, apply for credit fraudulently, and exploit personal data for scams. Potential Threat(s) If the Vulnerability Goes Unresolved: If Capital One had not addressed this issue quickly, further unauthorized access could have occurred. Additionally, the breach could have led to an increase in phishing attacks, legal penalties, regulatory fines, loss of customer trust, and long-term damage to the company’s reputation.

What Could a Developer Have Done to Prevent This Breach? A developer could have prevented this breach by implementing stricter security measures, including:

Regular audits of firewall configurations to identify misconfigurations.

Automated security alerts to detect and respond to unauthorized access attempts.

Applying the principle of least privilege, ensuring only necessary personnel had access to sensitive systems.

Using multi-factor authentication (MFA) to prevent unauthorized access.

Conducting frequent penetration testing to identify and fix security vulnerabilities.

Policies to Help Prevent This Type of Attack:

Implement strict access control and continuous monitoring.

Conduct regular security audits and compliance reviews.

Enforce cloud security best practices, including encryption and MFA.

Improve employee cybersecurity training to recognize security risks.

References

Chin, K. (2024, December 30). Biggest Data Breaches in US History (Updated 2025). UpGuard. Retrieved from https://www.upguard.com/blog/biggest-data-breaches-usChaurasia, N. (2024, December 18). 10 Biggest Data Breaches of the 21st Century. Sprintzeal. Retrieved from https://www.sprintzeal.com/blog/biggest-data-breaches