Author: Madhurima Rawat

Case Studies on Data Security Breaches

📌 1. Capital One Data Breach (2019)

🔍 **What Happened:**
Over **100 million customer records** were stolen due to a misconfigured AWS S3 bucket and firewall.

💣 **Why It Happened:**
A former AWS employee exploited a **server-side request forgery (SSRF)** vulnerability.

🧰 **Impacted Tools/Services:**

- AWS EC2
- AWS S3
- WAF (Web Application Firewall)

🛡️ **How to Prevent:**

- Implement strict **firewall rules**
- Regular **security audits**
- Enable **S3 access logging & IAM policies**

📊 **Real Impact:**

- 106 million users impacted
- Capital One fined **$80 million**

📌 2. Facebook Amazon S3 Exposure (2019)

🔍 **What Happened:**
Over **540 million Facebook user records** were found on publicly accessible Amazon S3 buckets.

💣 **Why It Happened:**
Third-party developers stored data insecurely without proper S3 permissions.

🧰 **Impacted Services:**

- Amazon S3
- Facebook APIs

🛡️ **How to Prevent:**

- Enforce **S3 bucket encryption and policies**
- Monitor **third-party integrations**
- Use **access control lists (ACLs)** wisely

📊 **Real Impact:**

- 540 million records exposed
- No major breach fines, but massive reputational damage

📌 3. Uber Cloud Leak (2016)

🔍 **What Happened:**
Hackers accessed **57 million user accounts** and Uber's GitHub repo containing AWS credentials.

💣 **Why It Happened:**
Developers **hard-coded AWS credentials** in public GitHub repos.

🧰 **Impacted Tools/Services:**

- AWS S3
- GitHub
- Uber user data

🛡️ **How to Prevent:**

- Never store **secrets in code**
- Use **environment variables** or **AWS Secrets Manager**
- Regularly rotate **keys and tokens**

📊 **Real Impact:**

- $168 million settlement
- Reputational damage

📌 4. Accenture Cloud Storage Leak (2017)

🔍 **What Happened:**
Critical infrastructure data was left exposed on **4 unsecured AWS S3 buckets**.

💣 **Why It Happened:**
Misconfigured permissions allowed public access.

🧰 **Impacted Services:**

- AWS S3
- CloudFormation Templates
- VPN Credentials

🛡️ **How to Prevent:**

- Use **Amazon Macie** to detect PII
- Regular S3 **bucket policy audits**
- Configure proper **IAM roles**

📊 **Real Impact:**

- No confirmed data theft, but highly sensitive info exposed

📌 5. Microsoft Power Apps Misconfiguration (2021)

🔍 **What Happened:**
Data from **38 million users**, including personal information, was accidentally exposed.

💣 **Why It Happened:**
Power Apps portals had **misconfigured default settings** exposing public APIs.

🧰 **Impacted Services:**

- Microsoft Power Apps
- Azure API endpoints

🛡️ **How to Prevent:**

- Enforce **default secure configurations**
- Periodic **config reviews**
- Automate **security baseline enforcement**

📊 **Real Impact:**

- 38 million records exposed
- Multiple enterprises affected (American Airlines, Ford)

📌 6. Tesla Kubernetes Breach (2018)

🔍 **What Happened:**
Hackers gained access to Tesla's **Kubernetes console** and used it to mine cryptocurrency.

💣 **Why It Happened:**
Console was left **unprotected**, and no authentication was required.

🧰 **Impacted Tools/Services:**

- Kubernetes
- AWS EC2
- Docker

🛡️ **How to Prevent:**

- Secure **Kubernetes dashboards**
- Apply **network policies**
- Enable **authentication/authorization**

📊 **Real Impact:**

- No customer data loss
- Infrastructure hijacked for cryptomining

📌 7. Code Spaces AWS Takeover (2016)

🔍 **What Happened:**
A DDoS attack led to the **total loss of business**, after an attacker deleted their AWS assets.

💣 **Why It Happened:**
Weak IAM security and no multi-factor authentication (MFA).

🧰 **Impacted Services:**

- AWS EC2, S3
- IAM
- Backup Systems

🛡️ **How to Prevent:**

- Enforce **MFA for root accounts**
- Backup off-cloud
- Principle of **least privilege**

📊 **Real Impact:**

- Code Spaces went out of business
- Total data loss

📌 8. Toyota Source Code Exposure (2022)

🔍 **What Happened:**
Toyota's T-Connect app source code was leaked due to **GitHub misconfiguration** revealing API keys.

💣 **Why It Happened:**
Developers pushed code containing **sensitive credentials** to public repositories.

🧰 **Impacted Services:**

- GitHub
- T-Connect Cloud APIs
- Customer info

🛡️ **How to Prevent:**

- Use tools like **GitGuardian**
- Implement **CI/CD secret scanning**
- Educate developers

📊 **Real Impact:**

- 296,000 users affected
- Apology issued, but no major fines

📌 9. Magecart CloudFront Attack (2018)

🔍 **What Happened:**
Magecart group exploited **CDN misconfigurations** to deliver malicious scripts.

💣 **Why It Happened:**
Poor **script validation** and lack of **subresource integrity** on cloud CDN.

🧰 **Impacted Services:**

- AWS CloudFront
- E-commerce websites
- Payment data

🛡️ **How to Prevent:**

- Use **Content Security Policies (CSP)**
- Enable **SRI (Subresource Integrity)**
- Monitor CDN updates

📊 **Real Impact:**

- Dozens of retailers affected
- Millions in card data stolen

📌 10. Twitch Data Leak (2021)

🔍 **What Happened:**
A 125GB torrent file was leaked including Twitch's **source code, payouts**, and internal tools.

💣 **Why It Happened:**
Weak server configurations and potentially **no segmentation** in infrastructure.

🧰 **Impacted Services:**

- AWS-hosted services
- Source control servers
- CI/CD pipeline

🛡️ **How to Prevent:**

- Harden cloud VMs
- Regular **penetration testing**
- Use **zero-trust architecture**

📊 **Real Impact:**

- 125GB internal data leaked
- Major PR fallout, Twitch acknowledged breach