**Top 10 attacks in Cybersecurity**

**1. Ransomware Attacks**

* **Company Example: Honda**
* **Details:** In 2024, Honda was reportedly hit by a ransomware attack that disrupted manufacturing and internal operations. The attack was attributed to the LockBit ransomware group.
* **Impact:** Operations were halted, affecting production and sales.

**2. Supply Chain Attacks**

* **Company Example: Uber**
* **Details:** Uber was targeted in a supply chain attack where attackers infiltrated a third-party vendor's systems to access sensitive company data.
* **Impact**: Personal data of users and drivers compromised, including critical infrastructure access.

**3. Phishing Attacks**

* **Company Example: Twitter (now X)**
* **Details:** In 2024, Twitter faced several phishing attacks targeting its employees and users, exploiting weak spots in social engineering tactics.
* **Impact:** User data stolen, compromised accounts.

**4. DDoS (Distributed Denial-of-Service) Attacks**

* **Company Example: Cloudflare**
* **Details**: Cloudflare, a major DDoS protection provider, faced a record-breaking DDoS attack in early 2024. The attack peaked at over 71 million requests per second, attempting to overwhelm their infrastructure.
* **Impact:** Disruption of services for several clients, potential data loss, and service instability.

**5. Zero-Day Exploits**

* **Company Example: Microsoft**
* **Details:** Microsoft’s Exchange Server was targeted by a zero-day exploit in 2024. Attackers used this vulnerability to gain unauthorized access to email servers across organizations.
* **Impact:** Data breaches, unauthorized access to email communication.

**6. Credential Stuffing Attacks**

* **Company Example: Facebook (Meta)**
* **Details:** In 2024, Meta (Facebook) was the victim of a large credential stuffing attack where stolen credentials from previous breaches were used to gain access to user accounts.
* **Impact:** Unauthorized access to social media accounts, identity theft.

**7. Advanced Persistent Threats (APT)**

* **Company Example: U.S. Government Agencies (via SolarWinds)**
* **Details:** Although it began in 2020, the SolarWinds APT attack still had ramifications in 2024. Hackers continued to target U.S. government agencies and private sector organizations.
* **Impact:** Stealthy access to government systems, data exfiltration, espionage.

**8. Malware (Trojans, Keyloggers)**

* **Company Example: Android Users**
* **Details:** In 2024, Android users saw a surge in Trojan malware on Google Play, often disguised as legitimate apps. Some apps were found to steal data or log user activity.
* **Impact:** Data breaches, loss of personal information, financial theft.

**9. Insider Threats**

* **Company Example: Tesla**
* **Details:** In 2024, Tesla experienced another insider threat attack where an employee leaked sensitive information about production and design to unauthorized parties.
* **Impact:** Theft of intellectual property, damage to competitive advantage.

**10. Cross-Site Scripting (XSS)**

* **Company Example: LinkedIn**
* **Details:** LinkedIn faced XSS attacks in 2024, where attackers injected malicious scripts into their platform’s website, affecting users who visited compromised links.
* **Impact:** Session hijacking, data theft, loss of trust among users.