|  |  |  |
| --- | --- | --- |
| **Problem** | **Cause of the Problem** | **Solution** |

|  |  |  |
| --- | --- | --- |
| **Facebook / WhatsApp / Instagram Outage (October 4, 2021)** | Configuration error in Facebook’s backbone infrastructure, leading to a DNS failure and server communication breakdown. | Facebook engineers identified and resolved the DNS issue. New internal monitoring systems were implemented to prevent recurrence. |

|  |  |  |
| --- | --- | --- |
| **Microsoft Exchange Server Vulnerabilities (March 2021)** | Zero-day vulnerabilities in the Microsoft Exchange Server software, exploited by attackers to remotely execute code. | Microsoft released security patches to fix the vulnerabilities. Companies were urged to update systems immediately, and security audits were recommended. |

|  |  |  |
| --- | --- | --- |
| **T-Mobile Data Breach (August 2021)** | Hackers accessed T-Mobile’s systems through a vulnerability in infrastructure, exploiting stolen credentials. | T-Mobile patched the vulnerability, and offered credit monitoring services to affected customers. Law enforcement investigated the breach. |

|  |  |  |
| --- | --- | --- |
| **Log4j Vulnerability (December 2021)** | A flaw in the Apache Log4j logging library allowed remote code execution, due to improper handling of user input. | Apache released an emergency patch (Log4j 2.16.0). Organizations scrambled to update affected systems. Regular scans and patching became critical. |

|  |  |  |
| --- | --- | --- |
| **Windows 10 Update Causing BSOD (April 2021)** | Compatibility issues with certain Intel RST drivers caused Windows 10 to crash with a Blue Screen of Death (BSOD) error. | Microsoft pulled the problematic update and released a patch to fix the driver conflict. Users were advised to manually rollback the update if necessary. |

|  |  |  |
| --- | --- | --- |
| **Uber Data Breach (September 2021)** | Compromised third-party vendor credentials allowed hackers to access Uber’s internal systems. | Uber initiated a security overhaul, including better vendor management and enhanced monitoring. The company also implemented stronger encryption and security protocols. |

|  |  |  |
| --- | --- | --- |
| **Google Cloud Outage (November 2021)** | Failure in Google’s IAM (Identity and Access Management) system disrupted authentication and access to services. | Google quickly resolved the IAM issue and restored service. A root cause analysis was conducted to improve system redundancy and reduce future outages. |

|  |  |  |
| --- | --- | --- |
| **Intel’s Alder Lake Chip Glitch (October 2021)** | Hardware scheduling issues in Intel’s Alder Lake CPUs caused performance problems with certain software. | Intel released firmware (BIOS) and software updates to address the issue and optimize system performance with Alder Lake processors. |

|  |  |  |
| --- | --- | --- |
| **Tesla Full Self-Driving Beta Bugs (2021)** | Incomplete AI training and unrefined software resulted in inconsistent performance and unsafe driving behavior in Tesla’s Full Self-Driving beta. | Tesla released several updates to improve FSD performance, refine AI algorithms, and added more real-world data training to enhance the system’s safety. |

|  |  |  |
| --- | --- | --- |
| **Amazon Web Services (AWS) Outage (December 2021)** | Bug in the AWS Kinesis service caused a widespread disruption in cloud services for multiple companies. | AWS deployed fixes to the Kinesis service. The company also conducted a full post-mortem review and implemented better redundancy and failover systems to minimize future outages. |