1. **MOVEit Data Breach (May 2023)**

|  |  |
| --- | --- |
| **Threat** | Exploitation of a zero-day vulnerability in the MOVEit Transfer software |
| **Vulnerability** | Unpatched software with unknown vulnerability |
| **Affected Security Pillars** | * Confidentality: Exposure of sensitive personal data * Integrity: Tampering of data during unauthorized access |
| **Risk Analysis** | Impacted over 77.2 million individuals and 2620 organizations including the US department of Enery and british Airways and  caused significant financial and reputational damage to affected entities |
| **Remediation Measure** | Regular software updates and conduction of security assessments to identify vulnerability |
| **Mitigation Strategy** | Implement a robust incident response plan to address breaches efficiently also employ IDS systems to monitor unusual activity |
| **Source** | https://dailysecurityreview.com/cyber-security/10-breaches-and-cyber-attacks-2023/ |

1. **Operation Triangulation(2023)**

|  |  |
| --- | --- |
| **Threat** | Targeted cyberattacks on IOS devices using a chain of zero-day vulnerabilities |
| **Vulnerability** | Unpatched IOS versions up to 15.7.x, with techniques effective up to IOS 16.2 |
| **Affected Security Pillars** | * Confidentality: Extraction of messages, passwords and tracking geolocation * Integrity: Manipulation of device data and functions |
| **Risk Analysis** | Thousands of victims, including commercial, governmental and diplomatic organizations. |
| **Remediation Measure** | Regularly update devices to the latest IOS version. |
| **Mitigation Strategy** | Conduct regular security audits and vulnerability assessments. Educate users on recognizing and avoiding potential phishing attempts |
| **Source** | https://en.wikipedia.org/wiki/Operation\_Triangulation |

1. **HTTP/2 Rapid Reset Vulnerability(Aug 2023)**

|  |  |
| --- | --- |
| **Threat** | Exploitation of zero-day vulnerability in the HTTP/2 protocol to launch large scale DDoS attacks |
| **Vulnerability** | Inadequate flow management in HTTP/2 protocol |
| **Affected Security Pillars** | Availability: Denial of service, rendering websites and services inaccessible |
| **Risk Analysis** | Disruption of major websites and services, including banks and social media platforms |
| **Remediation Measure** | Apply patches and updates to address the HTTP/2 vulnerability and implement rate limiting and traffic filtering to mitigate DDoS attacks |
| **Mitigation Strategy** | Deploy web application firewall to monitor and block malicious traffic. Establish redundancy and failover mechanisms to maintain service availability. |
| **Source** | https://blog.httpcs.com/en/biggest-cyber-incidents-of-2023/ |

1. **DarkBeam Cyber Attack(Sept 2023)**

|  |  |
| --- | --- |
| **Threat** | Unauthorized access to exposed Elastic search and Kibana interfaces |
| **Vulnerability** | Unprotected interfaces lacking proper security measures |
| **Affected Security Pillars** | Confidentiality: Exposed over 3.8 billion records, including email and passwords. |
| **Risk Analysis** | Reputational damage to DarkBeam as a cybersecurity firm. Potential phishing campaigns and identity theft using exposed data |
| **Remediation Measure** | Regularly audit systems to identify and rectify security gaps. Secure all the interfaces with appropriate authentication and access controls. |
| **Mitigation Strategy** | Conduct employee training on data protection and security best practices. Implement network segmentation to limit access to sensitive data |
| **Source** | https://dailysecurityreview.com/cyber-security/10-breaches-and-cyber-attacks-2023/ |

1. **Kia's vehicle management web portal Attack(Sept 2024)**

|  |  |
| --- | --- |
| **Threat** | Unauthorized access to vehicle control systems |
| **Vulnerability** | Inadequate input validation in Kia's web portal |
| **Affected Security Pillars** | * Confidentiality: Exposure of vehicle location data. * Integrity: Unauthorized control over vehicle functions. * Availability: Potential disruption of vehicle operations. |
| **Risk Analysis** | Potential for physical theft or unauthorized use of vehicles. Reputational damage to Kia, leading to loss of customer trust. |
| **Remediation Measure** | Conduct regular security assessments and penetration testing. Implement robust input validation and sanitization in web applications. |
| **Mitigation Strategy** | Ensure timely patching and updates of web application vulnerabilities. Adopt a layered security approach, including web application firewalls |
| **Source** | https://www.wired.com/story/kia-web-vulnerability-vehicle-hack-track/ |