|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | Payment Gateway System | | | | | |
| Area of Concern | Phishing attack(Unauthorized users into disclosing sensitive payment information) | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | Unauthorized user or group | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | The unauthorized user creates a fake payment portal or phishing email and take the sensitive payment information. | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Deliberate-The phishing attacks can steal payment credentials (credit card numbers, CVVs, Bank details). Attackers can use to commit fraud. Such as hacking or stealing money directly from insured accounts. And also they can sell deta | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | Use strong encryption to protect sensitive payment data during transmission and storage and can implement secure protocols for communication. And also can train users to recognize phishing attempts and understand the importance of not disclosing sensitive information. | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High**   **75%** | * **Medium**   **50%** | | * **Low**   **25%** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| A Phishing attack on payment gateway system could damage the company's reputation due to exposure of sensitive payment information, customer trust and unavailability could lead to user frustration.  Financial losses from fraudulent transactions, potential compensations to affected clients, and costs associated with rectifying the breach. | | | | Reputation & Customer  Confidence | | 5 | 3.75 |
| Financial | | 8 | 6 |
| Increased workload for investigating and resolving the phishing attack. | | | | Productivity | | 3 | 2.25 |
| Safety & Health | | 4 | 3 |
| Potential legal consequences and fines due to non-compliance with data protection regulations and failure to secure sensitive information. | | | | Fines & Legal Penalties | | 7 | 5.25 |
| User Defined Impact Area | | 0 | 0 |
| **Relative Risk Score** | | | | | | | | **20.25** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Administrative Controls | * Regular training programs to educate users on recognizing phishing attempts and safeguarding sensitive information. * Develop and maintain an incident response plan for handling phishing attacks. * Implement strict access control policies to limit access to sensitive payment information. | | | |
| Technical Controls | * Deploy advanced email filtering solutions to detect and block phishing emails. * Use strong encryption protocols to secure data in transit and at rest * Implement tools to detect and block phishing websites and fraudulent communications. | | | |
| Residual Risk | * Sophisticated phishing attacks that bypass detection tools. * Users might still fall victim to phishing attempts despite training. * New and emerging phishing methods that could exploit unforeseen vulnerabilities. | | | |

**Justification of probability and Severity values**

|  |  |  |
| --- | --- | --- |
| Attribute | Value | justification |
| Probability | 75% | Phishing attacks on payment systems are highly likely due to the valuable nature of sensitive payment data, and the increasing sophistication of phishing techniques. |
| Reputation & Customer Confidence | 5 | A successful attack could severely damage the company's reputation by compromising sensitive customer information, which could erode customer trust and loyalty. |
| Financial | 8 | Phishing attacks can result in fraudulent transactions, compensations, and recovery costs, leading to significant financial losses. |
| Productivity | 3 | Addressing the attack would consume significant internal resources, slowing down operations and affecting day-to-day productivity due to investigations and recovery efforts. |
| Safe and health | 4 | Although less direct, the stress and pressure from handling such attacks could potentially impact employee well-being. |
| Fines & Legal Penalties | 7 | There is a high risk of legal repercussions, including regulatory fines, due to non-compliance with data protection laws and the mishandling of sensitive customer information. |
| User Define Impact Area | 0 | No additional impact area has been identified for this scenario, indicating that the primary focus is on financial and reputational damage. |