|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Incident Reporting Form | | | | | | | | | | | | | | | | | |
| Personal Information | | | | | | | | | | | | | | | | | |
| Form No. (filled by Management) |  | | | | | | | Date | | | | | | | 11/27/2023 | | |
| Filled By: | Fayaz Khan | | | | | | | Time | | | | | | | 5.13 PM | | |
| Designation: | Lead DevOps & Compliance Engineer | | | | | | | Department | | | | | | | DevOps & Compliance | | |
| Incident Detail | | | | | | | | | | | | | | | | | |
| Date of incident: | Tuesday, 10 October 2023 9:00 pm | | | | | | | | | | | | | | | | |
| Time of Incident: | Tuesday, 10 October 2023 9:00 pm | | | | | | | | | | | | | | | | |
| Location of Incident: | New York | | | | | | | | | |  | | | | |  | |
| Reported by: | **First Name:** | | | Anees Ur | | | | | **Last Name:** | | | | | | | | Rehman |
| Email Address: | aneesr@nexelus.net | | | | | Phone Number | | | | | | | | | |  | |
| **Computer Network Defense Incident Type** | | | | | | | | | | | | | | | | | |
| Hardware | | | Software Failure | | | | | | | Network | | | | | | | |
| Data Loss | | | Physical Security Breach | | | | | | | Fire | | | | | | | |
| Data Theft | | | Building Damage Issues | | | | | | | Employees Issues | | | | | | | |
| Civil Unrest | | | Terrorist Activity | | | | | | | Malicious Code | | | | | | | |
| Known vulnerability exploit | | | Disruption of Service | | | | | | | Access Violation | | | | | | | |
| Accident or Error | | | Known vulnerability exploit | | | | | | | Others | | | | | | | |
| **Systems Affected:** | | | | | | | | | | | | | | | | | |
| Network zone affected | | Type of system affected | | | | | | | | | | Operating system | | | | | |
| Application | | Protocols or services | | | | | | | | | | Other | | | | | |
| Additional Details |  | | | | | | | | | | | | | | | | |
| **Computer Network Defense Incident Type (if applicable)** | | | | | | | | | | | | | | | | | |
| URL |  | | | | | | | | | | **Protocol** | | | | |  | |
| Malware |  | | | | | | | | | | | | | | | | |
| Additional Details |  | | | | | | | | | | | | | | | | |
| Classification Level | Confidential | | | | | | | | | | Location | | | | | Azure Cloud | |
| Description of Incident: | We encountered an issue with the backup jobs related to the two management jobs (Diff and Full). The maintenance plan included a daily run for Differential backups and a monthly run for Full backups. | | | | | | | | | | | | | | | | |
| Instant Actions Detail: | The problem stemmed from an expired encryption certificate, which was crucial for the proper functioning of the backup jobs. This expiration led to the generation of error messages, though unfortunately, these errors went unnoticed for some time. | | | | | | | | | | | | | | | | |
| Incident Details | | | | | | | | | | | | | | | | | |
| Data compromise | NO | | | | | | | | | | | | | | | | |
| System compromise | NO | | | | | | | | | | | | | | | | |
| Action taken: | Yes | | | | | | | | | | | | | | | | |
| Classification level of the information involved |  | | | | | | | | | | | | | | | | |
| Supporting documents attached (describe if any) |  | | | | | | | | | | | | | | | | |
| Incident duration | 1 Week | | | 2 Weeks | | | | | 3 Weeks | | | | | | | | 4 Weeks |
| 5 Weeks | | | 6 Weeks | | | | | 2 Months | | | | | | | | 3 Months |
| Incident Status | Resolved | | | | | | | | not resolved | | | | | | | | |
| Affected Organization Details | | | | | | | | | | | | | | | | | |
| Organization Name | All Clients | | | | | | | | | | | | | | | | |
| Type of Organization |  | | | | | | | | | | | | | | | | |
| Street Address |  | | | | | | | | | | | | | | | | |
|  |  | | | | | | | | | | | | | | | | |
| Reporting Detail (to be filled by management) | | | | | | | | | | | | | | | | | |
| Internal Reporting | Reported to: | | | | | | | | | | Tauseef | | | | | | |
| Designation: | | | | | | | | | | GM Development | | | | | | |
| External reporting | | | | | | | | | | | | | | | | | |
| External Authorities | Fire Brigade | | | | Police/ FIA | | | | | | | | | Rescue 1122 | | | |
| Ambulance | | | | Building Management | | | | | | | | | Bomb Disposal Squad | | | |
| Others (Specify) | | | |  | | | | | | | | | | | | |
| Actions Detail: | 1. **Identification of Issue:**   System-generated error messages were observed in various channels, including emails, Azure Alerts, and support notifications to Arshad, Asim, Tao, Peter, and Anees Ur Rehman.   1. **Analysis:**   Upon investigation, it was determined that the encryption certificate had expired, causing the backup jobs to fail.   1. **Renewal of Encryption Certificate:**   A prompt renewal of the encryption certificate was undertaken to restore the functionality of the jobs.   1. **Verification and Testing:**   The renewed certificate was applied, and thorough testing was conducted to ensure the jobs were functioning as expected. | | | | | | | | | | | | | | | | |
| Mitigation Details | In case of backup job or database service failure, following resources will be notified:  On first day of job failure email will be generated to:  1. Arif Khan 2: Anees Rehman 3: Fayaz Khan  On second consecutive day of failure, system will escalate the issue to following resources:  1. Tauseef Shahzad 2. Arshad Sadal 3. Asim Jameel  On third consecutive day of failure, the issue will be escalated to following resources:   1. Imran Rahman 2. Tao 3. Peter Platowski | | | | | | | | | | | | | | | | |
| **Root Cause Analysis (If required)** | | | | | | | | | | | | | | | | | |
| N/A | | | | | | | | | | | | | | | | | |
| Status of Mitigation Actions (If Any) | | | | | | | | | | | | | | | | | |
| Filled By: |  | | | | | | Designation: | | | | | |  | | | | |
| Department: |  | | | | | | Action Date: | | | | | |  | | | | |
| Details of actions: |  | | | | | | | | | | | | | | | | |
| Further Action Required? |  | | | | | | | | | | | | | | | | |
| Approval/Closing Details: | | | | | | | | | | | | | | | | | |
| Approved by: |  | | | | | | | | | | Date: | | | | |  | |
| Reasons for approval: |  | | | | | | | | | | | | | | | | |