|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Incident Reporting Form | | | | | | | | | | | | | | | | | |
| Personal Information | | | | | | | | | | | | | | | | | |
| Form No. (filled by Management) |  | | | | | | | Date | | | | | | | 2/22/2024 | | |
| Filled By: | Shafiq Ahmad | | | | | | | Time | | | | | | | 10.00 AM | | |
| Designation: | Network Administrator | | | | | | | Department | | | | | | | Networks | | |
| Incident Detail | | | | | | | | | | | | | | | | | |
| Date of incident: | Tuesday February 20, 2023 | | | | | | | | | | | | | | | | |
| Time of Incident: | 10:00 am | | | | | | | | | | | | | | | | |
| Location of Incident: | New York | | | | | | | Pakistan | | | | | | | | | |
| Reported by: | **First Name:** | | | Anees Ur | | | | | **Last Name:** | | | | | | | | Rehman |
| Email Address: | [aneesr@nexelus.net](mailto: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 | General VPN Connectivity Issue, which did not allow remote office to access servers. | | | | | | | | | | | | | | | | |
| **Computer Network Defense Incident Type (if applicable)** | | | | | | | | | | | | | | | | | |
| URL |  | | | | | | | | | | **Protocol** | | | | |  | |
| Malware |  | | | | | | | | | | | | | | | | |
| Additional Details |  | | | | | | | | | | | | | | | | |
| Classification Level | Confidential | | | | | | | | | | Location | | | | | Azure Cloud | |
| Description of Incident: | General VPN Connectivity Issue | | | | | | | | | | | | | | | | |
| Instant Actions Detail: | Pakistan telecom Authority put a ban on VPN connectivity without whitelisting specific IP address(es) of VPN Servers. | | | | | | | | | | | | | | | | |
| Incident Details | | | | | | | | | | | | | | | | | |
| Data compromise | NO | | | | | | | | | | | | | | | | |
| System compromise | NO | | | | | | | | | | | | | | | | |
| Action taken: | Yes | | | | | | | | | | | | | | | | |
| Classification level of the information involved | N/A | | | | | | | | | | | | | | | | |
| Supporting documents attached (describe if any) | N/A | | | | | | | | | | | | | | | | |
| Incident duration | Less than 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 | Nexelus Offshore office | | | | | | | | | | | | | | | | |
| 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:**   The offshore team was not able to connect to VPN for Server Connectivity   1. **Analysis:**   Upon investigation, it was determined that the Pakistan telecom Authority put a ban on VPN connectivity without whitelisting specific IP address(es) of VPN Servers.   1. **Whitelisting of VPN Server:**   A prompt request was forwarded to PTA for whitelisting of source and VPN IP Addresses.   1. **Verification and Testing:**   The users are able to connect with VPN Server and access remote servers | | | | | | | | | | | | | | | | |
| Mitigation Details | In case of changing static IP Address for office or VPN, a request will be sent to PTA for whitelisting new IP Addresses in Pakistan Office. | | | | | | | | | | | | | | | | |
| **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: | Arshad Sadal | | | | | | | | | | Date: | | | | | 2/24/2024 | |
| Reasons for approval: | VPN is connected and remote servers are accessed from all laptops/workstations. | | | | | | | | | | | | | | | | |