FGT5018.001 Cabling and junction boxes

Description: An adversary targets unprotected cables and junction boxes in order to disrupt service.

Fibers routed between pieces of equipment without proper protection are susceptible to damage, which can critically affect network reliability.

Labelling:

* Sub-techniques: N/A.
* Applicable Tactics: Impact

Metadata:

* Architecture Segment: PHYS & Env
* Platforms: Data transmission infrastructure and power supply
* Access type required: None
* Data Sources: Incident and event monitoring
* Theoretical/Proof of concept/Observed: Observed

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
| Disrupt service via physical damage | An adversary may damage cabling and junction boxes |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5005 | Compliance with cable standards.  Raceway / conduit is one of the easiest ways to protect any cable, fiber optic included. These hollow pieces of plastic act like a protective outer shell. |
| FGM5005 | Secure junction boxes.  Optical fiber junction boxes / splice closures shall be accessible to maintenance personnel and maintenance vehicles. A closure should be located away from high traffic or conditions that could cause damage to the closure or injury to personnel. [2] 11.2.3 advocates for cabling security |
| FGM5005 | Implement physical and environmental controls.  Sites should be provided with a full set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters |
| FGM5540 | Power supply facilities in the isolated area such as mobile base stations should preferably provide an uninterruptible power supply with capacity for all loading and capable of withstanding primary power supply failures for the duration of likely outages. If that is impossible, a mechanism to provide uninterruptible power to critical equipment should be installed. Batteries may need to be augmented with a private electric generator, especially in isolated areas. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Unprotected cables | Fibers routed between pieces of equipment without proper protection are susceptible to damage, which can critically affect network reliability. The fiber cable management system should therefore ensure that every fiber is protected from physical damage. |
| Unprotected junction boxes | Lack of protection of junction boxes / splice closures. Improper cable routing also causes increased congestion in the termination panel and the cableways, increasing the possibility of bend radius violations and long-term failure. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Data cables | Data cables used in the operator network infrastructure |
| Power cables | Power cables used in the operator network infrastructure |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5012 | Security Incident and event monitoring  Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. Additional considerations: development of use-case specific alert rules, integration and correlation of data at all levels (network, application), integration and correlation with service provider-level monitoring mechanisms. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Service unavailability | Destruction or damage of these assets may cause an unavailability of resources. |
| Information destruction | Destruction or damage of these assets may cause information destruction |

References:

|  |  |
| --- | --- |
| Name | URL |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, page 210, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| ISO/IEC 27011:(2016), “Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations” | https://www.iso.org/obp/ui/#iso:std:iso-iec:27011:ed-2:v1:en |