FGT5018: Vandalism of network infrastructure

Description: An adversary aims to destroy, expose, alter, disable, steal, or gain unauthorized access to physical assets such as infrastructure, hardware, or interconnection, affecting QOS or service availability.

Actions taken by actors aimed at destroying, disabling, or stealing physical assets supporting the 5G Network. A physical attack to 5G critical assets may disrupt, interfere, and ultimately cause unavailability of the network service. Despite the existence of physical protection mechanisms (e.g., physical surveillance and surveillance cameras, security locks, security guards), physical breaches and insider threat attacks may still occur.

Labelling:

* Sub-techniques: FGT5018.001, FGT5018.002, FGT5018.003, FGT5018.004.
* Applicable Tactics: Impact

Metadata:

* Architecture Segment: PHYS & Env
* Platforms: Physical
* Access type required: Physical
* 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 |
| Communication center | Unauthorized access, destruction of assets and impairment of operations |
| Telecommunications equipment room | Unauthorized access, destruction of assets and impairment of operations |
| Physically isolated operation areas | Unauthorized access, destruction of assets and impairment of operations |
| Equipment sited in other carrier's or partner's premises | unauthorized access, destruction of assets and impairment of operations |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| FGM5005 | Communications Centers.  Communication centers should provide a full set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. |
| FGM5005 | Telecommunications equipment room  Telecom equipment rooms should provide a risk-calibrated set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. |
| FGM5005 | Physically isolated operation areas  Remote equipment facilities should provide a set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters, taking into account its remoteness and lack of human presence. |
| FGM5005 | Equipment sited in other carrier's or partner's premises. Equipment located in third party facilities rooms should be protected using a risk-calibrated set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Improper physical security of 5G Core Components infrastructure | Improper physical security of Data-Centers / Telecommunication equipment room.  Improper isolation of physical secure perimeter between tenants.  Improper environmental protection controls.  Inadequate / defective security devices. |
| gNB component infrastructure | Improper physical security of telecommunications equipment rooms and equipment sited in partners’ or users’ premises.  Improper physical security of physically isolated operation areas.  Inadequate / defective security devices. |
| NFVI | Improper physical security of telecommunications equipment rooms.  Improper physical security of physically isolated operation areas.  Inadequate / defective security devices. |
| SDN | Unprotected Data Centre Interconnection channels areas.  Improper physical secure perimeter or isolation between tenants. |
| MEC host | Improper physical and environmental security of edge computing facilities  Improper security monitoring of edge computing facilities  Insecure service environment. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Physical infrastructure | Radio access units,  ICT equipment,  Light data center,  Cloud data center,  Edge Computing Facilities |

Detection

|  |  |
| --- | --- |
| **Id** | **Detects** |
| DS0040 | Asset tracking tools. Security Management and Detection |

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, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, November 2019. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks |

#doNotParse

1.1 POLICY CONTEXT

The present report was (??)