FGT5018.003 Edge Servers

Description: An adversary may seek physical access to isolated/remote edge servers using covert methods of entry with the intent to damage or destroy edge computing facilities, gaining unauthorized access at system level as an entry point to all hosted resources, theft of data on local storage, vandalism, and sabotage.

Edge computing facilities are, by their nature, seated in geographically distributed locations. Normally, the first choice will be communications shelters already operated by MNO. While communications shelters have physical security controls in place, these are calibrated to risks associated with communication equipment value. An additional risk assessment is needed to assess suitability in the context of additional risks incurred by presence of computing facilities and data.

Labelling:

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

Metadata:

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

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Damage edge servers | Adversary may obtain physical access to remote edge servers and cause damage to them. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5005 | Edge 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. Failure to do so may lead to unauthorized access, destruction of assets and impairment of operations. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Improper security monitoring of edge computing facilities | Mobile-edge computing have to be integrated in the network-wide Security Incident and Monitoring System, but with 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. Failure to do so may leave advanced or sustained threats undetected, as well as technical failures or malfunctions of local resources. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Edge facility equipment | Destruction of edge computing facilities, unauthorized access at system level as an entry point to all hosted resources, theft of data on local storage, vandalism and/or sabotage of equipment. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5012 | 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 of assets, unauthorized access, theft of data on local storage, vandalism, sabotage |
| 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 202, 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> |