SOLUTION DESCRIPTION

Advenica's secure filter & validation of measurement data in GIS

There is a risk that Operational Technology (OT) systems and their operations can be disrupted by threat agents targeting the data flows between IT and OT. With the right solutions, allowed data can flow between IT and OT without risking the sensitive OT environment.

Geographic Information Systems (GIS) can integrate with, and retrieve data from, systems for supervisory control and data acquisition (SCADA). This enables services and functionality based on real-time data produced by the SCADA system. In this process, data is collected from SCADA and transferred to a database from where the data is shared with other applications related to the GIS located in the office IT environment. Hence, there is a flow of data between the sensitive OT zone and the office/IT zone.

Challenge

Attack vector from IT to OT

Dataflows between IT and OT can potentially be exploited by threat agents trying to gain access to or disrupt the operation of the OT systems. This is particularly relevant when dealing with advanced threat agents such as foreign states or well financed and motivated cyber criminals.

IEC 62443

The standard IEC 62443 with focus on industrial cybersecurity states that: *"The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalisation defined in the risk-based zones and conduits model".*

This is a requirement for those who seek compliance with IEC 62443, and from a security perspective, a fully reasonable requirement when protecting any sensitive OT environment. So, this principle should be applied regardless of whether you seek compliance or not with IEC 62443.

Unhardened and unpatched servers

Standard Windows or Linux based platforms are widely used in OT environments today. Using these technologies

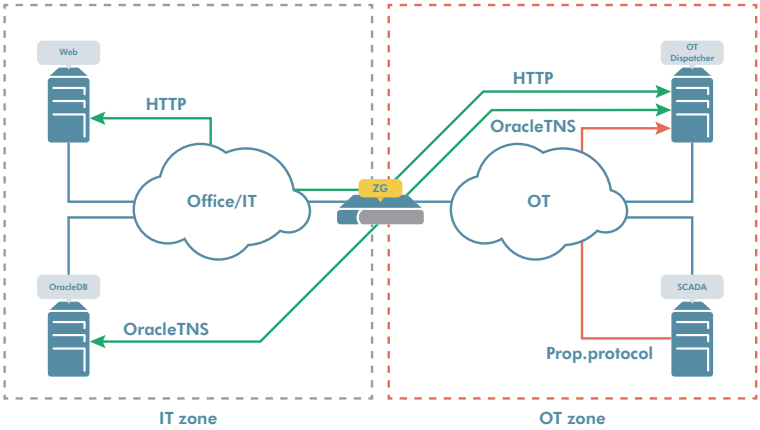
has some benefits but also require continuous maintenance and patching to stay resilient against the never-ending flood of new vulnerabilities and exploits. By exploiting vulnerabilities in the platform, application, or in any other services running in the machine, arbitrary code is executed, privileges are escalated, and consequently the machine is taken over. New attacks can thereafter be launched against SCADA and other OT systems.

Solution

Protect the OT service and machine with Advenica's ZoneGuard

The OT dispatcher service and server machine are protected using Advenica's ZoneGuard, a stand-alone device from the ground up developed as a security device with a hardened platform and defence-in-depth security architecture. Protocols used by the GIS application are HTTP and OracleTNS. The dataflows consisting of HTTP and OracleTNS traffic are validated making sure that only correctly formed protocol messages are exchanged. It is also assured that only an approved subset (as specified by the OT dispatcher service) of HTTP and OracleTNS traffic can enter or exit the OT zone.

ZoneGuard with HTTP and OracleTNS protocol validation services, validates traffic flow between the OT Dispatcher and the systems located in the IT zone



ZoneGuard will trigger an alarm and block any suspicious traffic and the hardened implementation in combination with its internal security architecture makes it very difficult for an attacker to get to the OT dispatcher server without being detected. From a defence-in-depth strategy point of view, we get another level of protection the attacker must penetrate to reach the OT zone.

Advantages

Defence-in-depth using Advenica's ZoneGuard technology

Protecting the OT server using ZoneGuard technology mitigates attacks against vulnerable protocol stack and service implementations. Attacks that could cause catastrophic consequences if spread to the ICS/SCADA environments. Also, policy-based filtering is applied to the content of protocol messages, assuring that only valid data is exchanged between IT and OT. The filter is customised according to organisational policy. This reduces the threat vector, i.e. possible paths or means an attacker can use to gain access to the OT servers. ZoneGuard supports hot standby mode and can be deployed in environments with requirements on high availability.

advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED