Are “Air Gap’s” realistic in today’s networks?

By: cuculan

Much has been written about the need to have Air Gaps installed between the IT and OT networks with the goal being to absolutely prohibit communication between these network segments. It is understandable that network managers would think along these lines given the relative insecurity of OT systems. Legacy systems abound with outdated operating systems, uncontrolled access, no built-in security, no segmentation etc. etc. all of which make these system prime targets for network intrusions. Indeed, in a lot of cases, operators do not have an accurate view of the inter-connectivity of these systems with each other or with the IT business systems.

So, an Air Gap looks like the absolute answer by prohibiting any communications between IT land and OT land. If one thinks purely from a security perspective, then that would be an obvious mitigation.

However, today’s world where the interaction between OT systems and IT systems has become a business differentiator based on the benefits derived from available operational data at a velocity that enables a business to glean critical information and react to operational events on a near real time basis.

To name but a few:

- Quality data that enables a business to understand the performance of its OT systems and potential impact of non-performing OT equipment
- Production data that enables the business to streamline logistics’ and supply chain processes to better support customers
- Maintenance data that enables the business to manage its production schedules based on its maintenance needs
- Engineering data that supports changes on how products are built or changes to product bills of material

There is, we believe, a strong argument that the business benefits of integrating IT and OT networks outweighs the potential vulnerabilities from a security perspective. If true, then networking professionals need to implement security solutions that provide the best protection.

So, what does this mean? Besides the basic blocking and tackling of anti-malware and anti-virus solutions it means that integration of IT and OT will require at a minimum:

- Minimizing the impact of any intrusion when it does occur by micro-segmenting your IT and OT network thus ensuring that any resource is only ever able to communicate with resources that it must communicate with and protecting against lateral breaches (East-West)
- Concealment of OT resources from the general IT network
- Two-way authentication to confirm that a source resource is authorized to communicate with a destination resource prior to communication AND that a destination resource confirms that communicated data is received from an authorized resource prior to accepting the communication
- Encryption of all data communicated between resources and ensuring that MITM and Replay attacks are recognized prior to acceptance of a communication
- User access control by ensuring that authorized users communicate through a protected resource and all other access is prohibited.

The reality is that IT and OT need to communicate. The reality is that there will be bad actors who intrude on these networks. If the business benefits are significant, we would argue that a hard separation using Air Gap's may not be the best answer and that security solutions built for OT environments should be considered.