How to make your data secure in a manufacturing environment

01 March 2022, 01:00

Annanda Rath
Christophe Michiels
Tatiana Galibus

Sirris has recently launched its cybersecurity service for manufacturing. As we start to reach out to companies through free intake or individual coaching, we receive more and more questions on how to protect data in manufacturing environments where machine and operation become more and more connected. Shielding data completely from cyberattacks is a complex task, but with several good security practices, it can help addressing large parts of the issue.

There is no one-fits-all solution, the selection of data protection solutions depends largely on the system's architecture, machine's capability, and protocols used. However, there are the general security rules, that, if implemented, can help reducing the risk to data breach.

- The first important strategy to consider is to **implement access control to data**. Applying 'least privilege' principle, which means, allowing the minimal level of rights, that allows the user to perform his/her role. Data that is not meant for users should not be accessible to them. This can help preventing unnecessary access and use of data. Standard access control protocol should be used when possible. In the event that legacy machines are in operation (only traditional username & password is possible) and advanced access control technology such as multifactor authentication is not available, a good password management practice is necessary (e.g., password policy & its renewal, …). One password for all (e.g., one password for multiple machines) should be avoided and password must be kept safe. Use password manager if you need to manage multiple passwords for different accounts or machines. There is plenty of password manager software both open source and proprietary (e.g., KeePass, Bitwarden, …).
  Data also needs to be classified according to its level of confidentiality and highly confidential data requires stronger security protection. When it comes to defining the access control policy to those data, the user's role in an organisation (company) is used as a condition for granting access. For example, there should be a separation of data in different categories, such as, financial data, employee data, operational data (from machine & on-premises communication) and intellectual property (IP) data.

- A second strategy is to look at **the protection of data at rest**. Generally, in a manufacturing environment, a large amount of data is produced by machines and is kept in data-historian storage. This data needs to be kept secure at all times and it also needs to be made accessible for analysis. There are different solutions for data-historian protection, it depends on whether the storage is on-premises or in the cloud. However, the general rule is that for important or highly classified data, it needs to be cryptographically protected before storing.

This adds another layer of protection to the access control highlighted above. The data to be in storage should also be scanned before storing to ensure that it is virus- or malware-free. Multiple copies of data should be kept secure in different places to reduce the risks in the event that data is corrupted or hacked (e.g., ransomware). When backing up data, a 3-2-1 backup strategy should be used (3 copies of data (production data and 2 backup copies) on two different media (disk and tape) with one copy off-site for disaster recovery.

- A third strategy is to look at **data security in transit**. This includes secure data exchange and sharing on-premises or between sites through a public network (e.g., the Internet) or with a third-party system (e.g., supply chain or contractor). Data exchanged on-premises also need to be protected by using a secure/encrypted communication channel (e.g., TLS or DTLS, …) when it comes to moving data from one place to another (e.g., between networks) on site. If data needs to be sent through a public network, it is recommended to use VPN or zero-trust technology, to establish a secure tunnel for sending or exchanging data.

- With advanced and sophisticated hacking tools, attackers can always find a venue to get into the network/system, regardless how strong the security we have in place. Attacker can access data without our knowledge. Thus, it is vital to have **a data access monitoring tool**. This tool allows us to monitor user data access activities and provides an on-time alert in case any anomaly is detected. Commercial tools such as Microsoft 365 and OneDrive offer an audit log, which can be used to check/follow-up data access and sharing activities in the platform.

Authors

Annanda Rath

Christophe Michiels

Tatiana Galibus