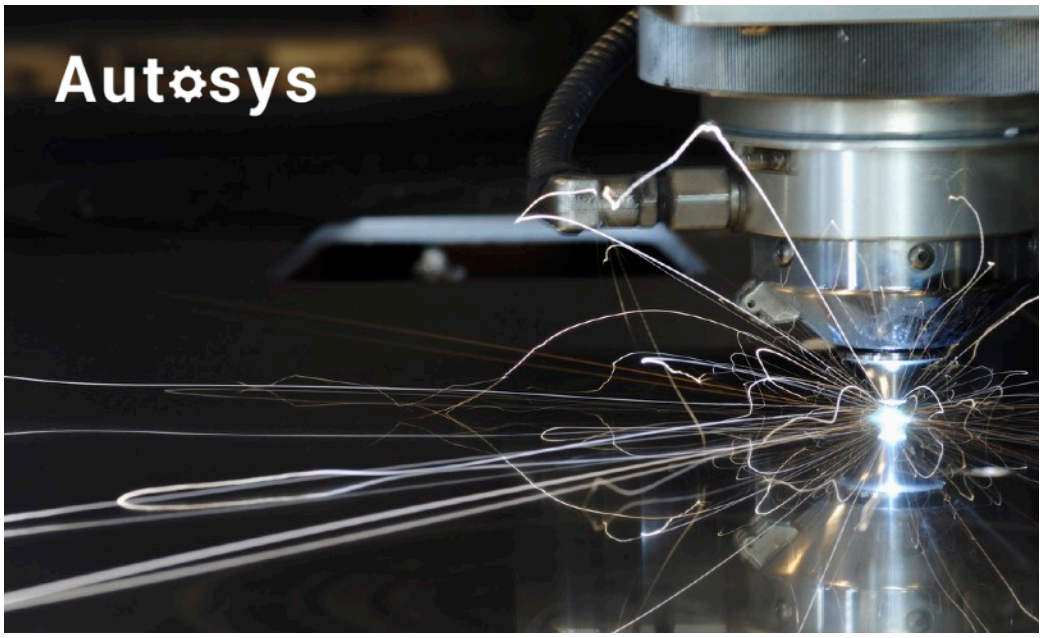
AUTOSYS INDUSTRIAL SOLUTIONS PRIVATE LIMITED 14 DECEMBER 2022

Quad Newsletter

Cybersecurity in your digitisation journey



Understanding cyber security

Is your company network secure? Could your machines be an entry point to your network exposing you to vulnerabilities?

Smart factories will result in improved productivity and more efficient, streamlined factory operations it will also open up an ocean full of opportunities, including updating old machines systems and connecting legacy systems with sensors and edge gateways. On the other side it opens up an unexplored vulnerability and exposes large amounts of data to cybercriminals and increases cyber security threats. The overall impact could be catastrophic. It has become important to deploy systems in place to avoid potential leaks that could be from company network to machines controllers.

1

LIMIT DATA ACCESS

Limit the data that can be transferred out of the company network

2

FIREWALL & POLICY

It is crucial to have a cybersecurity policy along with data policy of the company

3

SECURE NETWORKS

Deploy necessary firewalls and enforce the policies across

Carry out risk assessment
Conduct regular audits to be aware of various vulnerabilities

Don't overlook mobile devices
Keep a close look on mobile devices, restrict information flow on the same

Vigilance on third parties
Ensure there is necessary cover on data shared with third party vendors

Look at your machines
Your machine controllers/ PLCs could be an entry point into your OT networks

Restrictions on files outside of organisation network
Cyber scans that shall scan through the files sent outside the company network for various keywords before they are sent

Plant security lookup!

"Global spending on the digital transformation is forecast to reach $2.8 trillion in 2025" - International Data Corporation

Every new device deployed creates a vulnerable entry point into the operational technology network. A company must employ necessary processes to conduct regular, comprehensive audits on the operational and information technology networks at the plant level.

One must identify and create a register of all the assets that could pose an entry point into either operational or information technology networks and identify various risks and vulnerabilities on exposure of the same.

Ensure the company has focused on developing a cybersecurity policy and it is important to communicate the same across the organisation. One must have various checks and balances in place to ensure that the risks and consequences at differential levels. A close monitor on certain types of documents that could be filtered through the firewall if they are sent outside the company network. These must create necessary red flags within the system and highlight these transactions. A lot of companies are unaware of the different protocols that are employed within the organisation over which information could be transmitted. It is essential to maintain a comprehensive document of the different protocols and how any potential risks could be mitigated over them.

This will require the company to deploy a threat detection software that could operate in realtime providing constant vigilance against any unwanted or unauthorised requests.

An incremental approach where various layers are incepted and and deployed phase wise is essential. It is impractical to expect overnight advancements and vigilance. Each layer shall act as a foundation to the subsequent layer and thereby the policies and security can be built on.

LOOK BEYOND THE NETWORKS, HARDWARE TOO?

While you need to be vigilant of hackers trying to get into your networks, don't forget that your hardware can be stolen too. Unauthorised individuals should be prevented from gaining access to such devices. This may include physically securing the device or adding a physical tracker to recover the device in case of loss or theft. Ensure the entire organisation understands the importance of any data that might be stored on their cell phones or laptops when out and about. **It's also a good idea to set up remote security – this allows you to remotely delete the data on a lost hardware.**