CYBERSECURE IN 7 SIMPLE STEPS

Even though there's no silver bullet for cybersecurity, there are some steps each business should take to boost resilience. With this short guide explaining seven steps to cybersecurity, we aim to help you get the basics in order and inspire you to give cybersecurity the attention it deserves.

sirris

driving industry by technology

STEP

1

DOCUMENT THE NETWORK CONNECTIONS AND EXPOSURES

A fully connected shopfloor maximises efficiency by integrating smart manufacturing machinery, AI-powered automation, and advanced analytics.

However, when your entire shopfloor is connected, this poses some cybersecurity risks: when hackers get access to one component within your network, they can take over the whole shopfloor.

That's why it's crucial to, first of all, map your entire network. Consider every connected robot, laptop, machine, or printer, so you know exactly what devices or connections are in danger when things go wrong.

When documenting your network connections and exposures, keep in mind wireless live network access points, connectivity points, isolated points, legacy machines and office devices.

STEP

2

SET UP SECURE NETWORK ARCHITECTURE

Once you have mapped every connected component to your network, you can set up a secure network architecture by grouping devices and building solid firewalls. With a well thought out network set-up, you can segregate devices and prevent lateral movement in case your network gets unwanted visitors.

A first step is to isolate IT and OT. This way, you make sure that when, for example, one of your employees gets their office device infected, your machinery is safe, and production can keep running.

Optimise your network architecture by creating different groups of devices and access points within your network map, protecting them with solid firewalls.

STEP

3

CONFIGURE NETWORK VISIBILITY AND MONITORING

Network visibility is the concept of being aware of everything moving within and through your network. When you have a clear idea of what is typical behaviour or what should be happening, you can set a standard for what's normal.

By monitoring everything that happens in your network, you can easily identify behaviour that deviates from the standard. This way, you can quickly spot performance issues, cyber-attacks or other vulnerabilities. Such anomaly-based threat detection helps you distinguish problems even before they become one. After all, a successful defence strategy can fight off a threat before they cause any damage.

STEP

4

SECURE THE REMOTE CONNECTIVITY AND MAINTENANCE PROCEDURES

A lot of the time, an essential aspect of digitalisation is remote access to industrial facilities. Remote connectivity can significantly improve operations efficiency, for example, because fewer people need to be present on-site 24/7 to ensure continuity. However, any external access is a potential vulnerability for cyber-attacks.

That's why it's vital that when parties should be able to connect to your industrial facilities remotely, they can do so in a secure way. Technologies like VPNs, intrusion prevention systems, SASE, firewalls, zero trusts and IAMs can offer a solution here.

STEP

5

ENHANCE AUTHENTICATION AND REMOTE ACCESS SECURITY

Passwords are an easy solution to keep unwanted visitors out of your network. However, passwords that are too easy to guess, default passwords or passwords shared between various people instead of personal passwords for each individual, are no longer a reliable form of network protection.

An additional step in your remote security policy can be to centralise authentication where possible, for example via AD or LDAP. You can also ensure authorisation (is this person allowed access to this resource?) or use multi-factor authentication by, for instance, double-checking their identity.

STEP

6

REGULARLY IMPROVE AWARENESS AMONG STAFF

The IBM Cyber Security Intelligence Index Report claims that 95% of cyber security breaches are primarily caused by human error. That doesn't mean that your employees are your cybersecurity policy's enemy, but it does mean that you should invest in a cybersecurity culture (CSC).

Awareness training is invaluable here. We think that at least once a year, every manufacturer should carry out training which covers relevant company policies such as IT/OT security, information security, and physical security. When your staff is aware of the risks and the possible consequences of their behaviour, they most likely will adapt their ways to protect your company's safety.

STEP

7

ASK SECURITY QUESTIONS TO PROVIDERS

Nowadays, most companies depend at least partially on external service providers. Whether it's for data management, marketing, logistic operations or any other business aspect, these service providers often have some kind of access to a company network or company info.

That's why it's essential to carefully consider each external party before you exchange any kind of information. Don't hesitate to ask questions about their own cybersecurity policy, connection details and parameters, network visibility, network protocol and segmentation, credentials control, data security, etc.

Any questions?

Would you like to start a personal cyber security journey with our experts? Don't hesitate to contact us!

TATIANA GALIBUS
Cyber Security Ambassador
+32 493 31 15 76
tatiana.galibus@sirris.be

sirris
driving industry by technology