During an IT/OT emergency, using IT/OT contingency plans and processes that have never been tested is as effective as improvising

Cyber security exercises are for training your employees, from management level to the IT administrator. They expose you to realistic situations that can actually occur in everyday operations. The insights gained from these scenarios are among the most important prerequisites for appropriate planning and action.

Vulnerabilities are detected and resolved

During the exercises, we will work with you and your employees to test existing processes, measures and plans. We will show you potential weaknesses and find ways to optimise your incident response plan. This will considerably increase your knowledge of IT/OT threats and will make taking action in the event of emergency more routine.

Significant time savings when incidents arise

Your processes, measures and plans will probably contain undetected omissions or mistakes. These will be uncovered during cyber security exercises. At the same time, we will find and develop solutions on how to avoid such failings in the future. After solving these vulnerabilities, you will soon see significant reductions in the time it takes to detect, respond and recover.

Routine cyber incident handling and more secure handling

Arguably, the most important aspect of process optimisation is identifying the needs for action at the technical, organisational, infrastructural and personnel levels. The goal here is to limit possible damage and ensure that normal operations are quickly resumed after an incident.

To do this, you must clearly identify the people in your incident response team responsible for making decisions in each area. This will allow the person concerned to precisely adapt and take immediate action as the go-to person and coordinator in the event of an emergency. Your defences and tools will be optimised and you will also improve your cyber incident handling capabilities in terms of situation assessment, development of possibilities for action, business continuity, and resumption and follow-up.

All this results in more routine action and more secure handling. In addition, our exercises enhance cyber security leadership and decision-making abilities, and ensure better and clearer communication between teams.

AIRBUS

Cyber Security Exercises

During an IT/OT emergency, using IT/OT contingency plans and processes that have never been tested is as effective as improvising

Your benefits at a glance

- Testing and optimising existing IT/OT emergency documents and processes
- More routine actions to take in emergency situations
- Improved team and decision-making skills
- Time savings through reduced time to detect, respond and recover

Our modular approach:

Functional test

Our functional tests check the technical components, procedures and sub-processes for their functionality as defined in the various incident handling sub-plans. These include, for example, tests of redundant lines, power supply, data restoration or the signalling technology applied.

Cyber incident handling workshop

This workshop is for thinking through problems and scenarios theoretically. The cyber incident handling processes are analysed based on realistic scenarios. Participants review the plans theoretically and verify the plausibility of the content and assumptions made. This validation can reveal mistakes and discrepancies.

Simulation exercise

The simulation exercise provides training in cooperation between the IT/OT emergency team and the operational teams in a realistic emergency situation. The processes and measures defined in the contingency plans, such as alerting, assessment, escalation, emergency measures and resumptions, are also practised operationally.

Depending on the scenario, external bodies such as authorities, the fire brigade and aid organisations may also be involved in the exercise.

These various cyber security exercises serve to validate plans and processes and can reveal inconsistencies and mistakes before costly operational expenses are made.

What is the extent and scope of exercises you are looking to do with us?

AIRBUS

FRANCE
Metapole 1, boulevard Jean Moulin
CS 40001 / 78996 Elancourt Cedex
France

GERMANY
Willy-Messerschmitt-Str. 1
82024 Taufkirchen /
Germany

UNITED KINGDOM
Quadrant House / Celtic Springs
Coedkernew / South Wales
NP10 8FZ / United Kingdom

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com