V CONFERENZA NAZIONALE

Partenariato cybersecurity privacy

Cybersecurity: stato dell'arte, sistemi di difesa e resilienza

Roma, Palazzo Wedekind, Piazza Colonna 366, 4 aprile 2022

ICS cybersecurity and cyber range

Salvatore D'Antonio

ICS users and cybersecurity

- Historically, Industrial Control Systems (ICS) were physically isolated or air-gapped from the outside world.
- Now systems are connected to the corporate WAN and the Internet to allow remote process monitoring and maintenance
- ICS are built on proprietary hardware and software
  - Incompatible or unknown reaction to cyber-security patches. ICS often operate with out-of-date software
  - IT-based solutions, such as firewalls, are not familiar with ICS communications protocols
- The focus is on keeping the process running
  - Cybersecurity can add a point of failure, disrupt the process, and make maintenance more difficult

ICS users and cybersecurity

- Control engineers, technicians, operators typically are not skilled in cybersecurity. Conversely, IT professionals are not skilled in process control.
  - They have different, and sometimes conflicting goals in the corporate structure
- It is difficult to make a business case for cybersecurity, though this is improving. The perception is “no attacks mean no problems”

Cyber Range approach

- Testing the resilience and cybersecurity features of a real system represents a complex problem, mostly for industrial control systems as the consequences in the event of an accident can impact human health and environment

- ➢ Cyber Range platform can simulate/emulate realistic and complex scenarios for cybersecurity operations and resilience testing

What is a Cyber Range ? (from NIST Guide)

- Cyber ranges are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet-level environment
- They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing
- A cyber range may include actual hardware and software or may be a combination of actual and virtual components. Ranges may be interoperable with other cyber range environments
- The Internet-level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer

Cyber Range functions

- Internet Services simulation
- Attack simulation
- User activity simulation
- Scenarios and content development
- Competency management
- Data collection and analysis
- Scoring and reporting

Cyber Range strengths

CYBER RANGE CAN..

- REALISTICALLY REPRESENT OPERATIONAL ENVIRONMENTS AT DIFFERENT LEVELS OF SECURITY, FIDELITY, AND/OR SCALE
- ALLOW TEAMS TO WORK TOGETHER TO IMPROVE TEAMWORK AND SOLVE COMPLEX CYBER PROBLEMS
- PROVIDE PERFORMANCE-BASED LEARNING AND ASSESSMENT
- PROVIDE AN ISOLATED ENVIRONMENT TO TEST ADVANCED CYBER SECURITY TACTICS, TECHNIQUES, AND PROCEDURES
- SIMULATE ON-THE-JOB EXPERIENCE

Cyber range for training/education

- Educators can use cyber ranges to organize classroom courses, instruct or assess students
- Students can use cyber ranges to apply knowledge in a simulated and secure environment and develop cyber security skills
- Organizations employees can learn security best practices and exercise on realistic environment scenarios

Key facts

- According to the World Economic Forum (WEF) Report 2021, there is a global gap of over 3.12 million cyber security workforce, with two million in the APAC region alone.
- Gartner predicts that by 2022 15% of large enterprises will be using cyber ranges to develop the skills of their security teams.