SUCCESS CASE

CYBER RANGE: PROMOTING CYBERSECURITY AWARENESS

JULY 2020 | Nº10

INTRODUCTION

Cybersecurity plays a vital role in digital transformation. The key strategies for fighting an invisible enemy that can attack at any time, using any digital device, causing severe damages to the organization are: raise awareness, encourage preparation, and spread information. Sensitive to this fact, EDP is set to build a strong defence that counts on every coworker. Investment in transformative technologies can be meaningless if the business, its customers and other vital assets are not appropriately protected.

MAIN CHALLENGES

EDP's investment in digital transformation was materialized in new processes and product development at a new and improved speed. At the same time, it also highlighted the importance of promoting cybersecurity practices throughout the company.

However, the complexity and speed of digital development continues to challenge even the most extensive security operations. Attentiveness and readiness are crucial to prevent and mitigate the possible consequences of these types of threats and to maintain a safe environment for the company's stakeholders. An awareness-raising strategy has, therefore, become crucial to successfully address cybersecurity challenges.

SOLUTION

Cyber Range is a cybersecurity awareness initiative, created by EDP. Launched in 2016, this program has two main goals: raise awareness among as many EDP coworkers as possible so they know how to identify a cyberattack, both at work and at home, and also to provide them with the right tools and information to prevent a possible reoccurrence. EDP's Cyber Range is based on a one-of-a-kind infrastructure that has three different purposes:

- **A Security Lab**. Where new equipment, software and security protocols are put to the test regarding their ability to resist cyberattacks;
- **A Cybersecurity exercise arena**. Either in cooperation with external partners or internally, Cyber Range offers a realistic environment for conducting cybersecurity tests, boosting the company's skills in detecting and reacting to a cyberattack;
- **A Training academy**. Cyber Range's main effort is to train as many coworkers as possible in how to spot and how to respond to a cyberattack, particularly those working in IT and critical energy facilities.

Four specific training sessions have been designed to provide trainees with a complete and realistic experience. In a simulated physical scenario, participants learn what it's like to be under a cyberattack and what can be done not only to mitigate it, but also to prevent future incidents.

338 PHISHING CASES
in 2019

204 TRAINED COWORKERS
in 2019

1.800 SECURITY INCIDENTS
per year are handled by SOC

About Digital Global Unit (DGU)

Digital Global Unit (DGU) was born to help EDP Group drive transformation to digital by developing outstanding ideas to improve and optimize processes and thus simplifying both clients and employees' journey. Comprised of a multifaceted team of developers, engineers, designers, data scientists, and other experts, DGU works every day to turn impossible ideas into successful business projects at EDP Digital Factory.

EDP - ENERGIAS DE PORTUGAL SA
Digital Global Unit (DGU)
Av. 24 de Julho, 12 - Lisboa
dgu@edp.pt

digital global unit

SUCCESS CASE

HOW IT WORKS

E-LEARNING

To reach as many EDP coworkers as possible, Cyber Range is preparing to launch its cybersecurity courses online.
This way, it will be possible for more people, whatever their location, agenda, or availability, to access and benefit from the knowledge shared in these sessions, thus reinforcing the company's defence against digital threats.

CONTINUOUS IMPROVEMENT

Cyber Range is continuously looking for new ways to improve learning content and methods. To accomplish this goal, the team promotes learning groups with different backgrounds, collects trainees' opinions, and tests new learning methodologies.

SIMULATION

After the academic part, trainees are challenged to monitor, detect, and solve a cyberattack in a simulated scenario featuring an electrical distribution substation, a thermoelectric powerplant and the IT systems needed to support and remotely operate these critical infrastructures. The simulation comes in different forms, such as a cross-site scripting or a port-scan attack, but, whatever form it takes, participants have to work as a team to come up with a solution and a prevention strategy.

TRAINING

There are four different courses available. One general course that targets basic cybersecurity concepts, available for any coworker and one lighter course for team managers that highlights the implications of cyber-attacks. Additionally, there are two specialized training courses aimed at preparing specific EDP professionals responsible for operating critical energy infrastructures. Accessible to the entire EDP universe, the length of the training courses depends on their complexity and target audience.

BENEFITS

- Cultural change regarding cybersecurity issues. By raising awareness, EDP is fostering a safer digital environment;
- EDP's increased power to stop, solve, and prevent; cyberattacks;
- Responsive content production. Aside from the core learning materials, the Cyber Range team is creating awareness materials, spreading knowledge throughout the company;
- Increased cyberattack reporting.

CYBERSECURITY BEST PRACTICES

Be cautious about suspicious emails
When receiving an email, always check its origin before opening enclosed documents or clicking on links.

Keep your PC locked
Whenever you are away from your computer, keep it locked. Use the Win + L shortcut.

Use strong passwords
Create passwords with letters, numbers, special characters, and upper-case letters. Change your password frequently and don't reuse old passwords.

Backup!
Ensure you can access your information even in the event of a cyberattack through regular backups using OneDrive.

Never illegally download
Illegal downloading activity significantly increases the risk of exposure to malware.

Social media restraint
Be aware of what you publish on social media. Post with restraint to avoid becoming an easy target.

Report suspicious activity
EDP's specialized Security Operations Center is ready.
If you discover any suspicious activity or a suspicious email in your inboxes, immediately report it to the EDP cybersecurity team at the Security Operations Center. The faster they know about the threat, the faster they will deal with it and protect the organization.