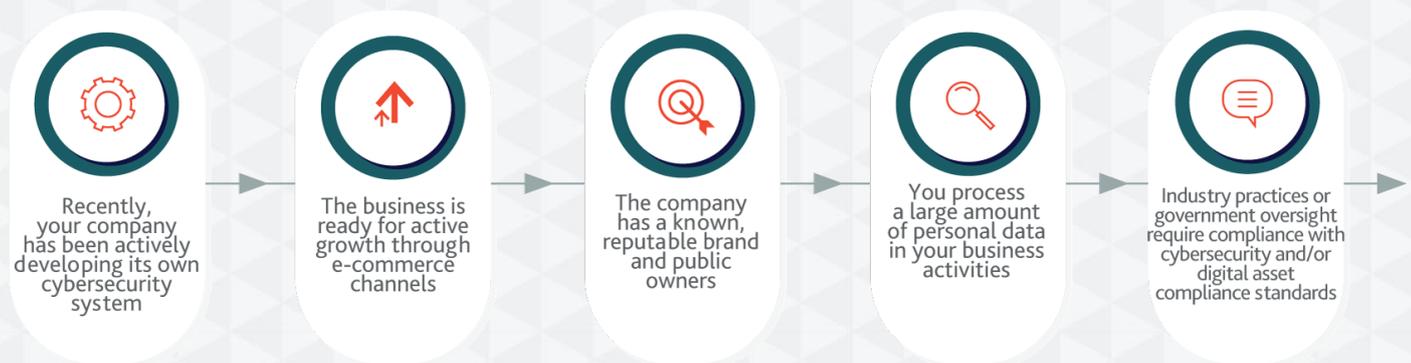


BDO IN UKRAINE OFFERS CYBERSECURITY SERVICE FOR CORPORATE NETWORKS

Reputable sources point that the total number of cybercrimes due to the COVID-19 pandemic has increased by an enormous x7 times! Unfortunately, Ukraine is part of this horrible statistic, because only in our country any corporate network can be attacked through 2,7 million open ports (vulnerable hosts). And almost 3,000 databases with personal data are already in the public domain and can be used by anyone. Meanwhile, there has been a lot of distressing news

last year about the malicious cyberattacks that initially encrypt some elements of infrastructure (e.g. routers), and then blackmail business with further demand of crypto payments. Till now a lot of well-known Ukrainian companies had such negative and expensive experience, while cyber-criminals weren't properly punished or even detected. In the same time corporate business continued to suffer greatly in monetary and reputation terms.

If your company or business:



then, most likely, your corporate network is very attractive for hacker attacks, and therefore needs to be tested for resistance to targeted threats.

PENETRATION TESTING

WHAT IT IS?

A method of assessing the readiness of the company's IT infrastructure to protect against external threats, which fully simulates the potential attack of cybercriminals. A team of IT specialists plays the role of hackers trying to hack the system, having agreed it in advance with the corporate network owners, by using all possible vulnerabilities of the system.

HOW DOES IT WORK?

Our experts will try to penetrate the company's internal network by simulating of hacker attack. This ethical intrusive test will explore:

- ▶ effectiveness of internal infrastructure protection
- ▶ vulnerability of WI-FI equipment
- ▶ risk analysis of lost / stolen remote devices
(simulation by using any customer's laptop)*
- ▶ effectiveness of using cyber vulnerabilities, identified during the attack



* Exclusive offer from BDO in Ukraine

HOW IT CAN HELP YOUR BUSINESS?

To test readiness of your existing cybersecurity system in real-life conditions

To practice security scenarios while intrusion attempt is running

WHAT IS THE RESULT?

1 Detailed technical report on identified cybersecurity vulnerabilities and executive summary for senior management



Standards used:
PTEST, NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OSSTMM, BSI, SANS TOP 25



Report standards:
Common Vulnerabilities and Exposures (CVE) Compatible, Common Weakness Enumeration (CWE) Compatible, Common Vulnerability Scoring System (CVSSv3.1)

2 Running another penetration testing after found vulnerabilities elimination (included in the offer)

Interested?

Contact us:



ANDRII BORENKOV
Head of Advisory

✉ aborenkov@bdo.ua
☎ +380 50 380 96 01

BDO in Ukraine

🌐 www.bdo.ua
✉ info@bdo.ua