BDO RISK ADVISORY SERVICES
PENETRATION TESTING

AN ETHICAL ATTACK ON THE REMOTE WORKING ENVIRONMENT OF YOUR ORGANISATION

Cyber threats are constantly growing in size and complexity. In the last couple of days, the world has witnessed an increase in cyber-attacks. Hackers are aware that due to the COVID-19 crisis, many people are actively working remotely. As an organisation, are you therefore certain that the technology that you have put in place, which facilitates remote working, has been rolled out correctly and offers adequate protection against attackers? Penetration testing of your remote working environment by experienced ethical hackers is the best method to get a good and independent view on the actual state of your IT infrastructure and application landscape security.

In order to identify the technical IT security risks, multiple scenarios are possible. Penetration testing is performed in white, black or grey box scenarios.
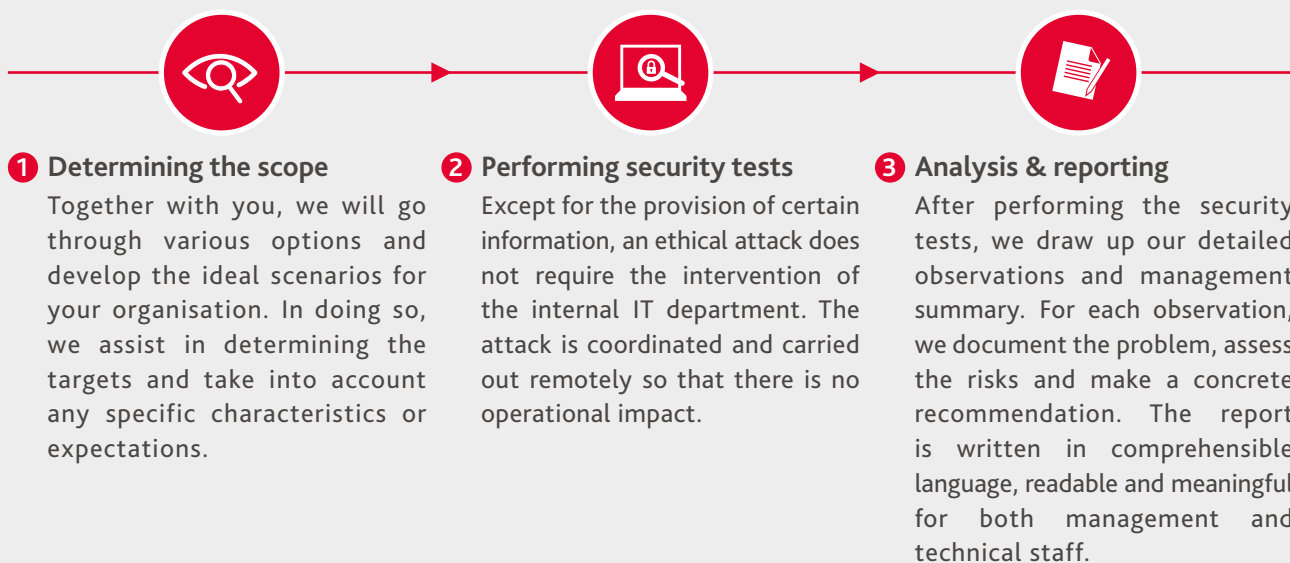
WHITE BOX | An attack carried out on the basis of prior knowledge such as log-in details or other relevant information to test more specifically on certain domains.

BLACK BOX | An attack without prior knowledge of the environment.

GREY BOX | An attack with limited prior knowledge of the infrastructure, in which the extent to which more information about the target can be found is investigated.

Our ethical attacks are conducted on the basis of best practices, appropriate tools and specific expertise in accordance with (international) standards.

OUR APPROACH

1 Determining the scope
Together with you, we will go through various options and develop the ideal scenarios for your organisation. In doing so, we assist in determining the targets and take into account any specific characteristics or expectations.

2 Performing security tests
Except for the provision of certain information, an ethical attack does not require the intervention of the internal IT department. The attack is coordinated and carried out remotely so that there is no operational impact.

3 Analysis & reporting
After performing the security tests, we draw up our detailed observations and management summary. For each observation, we document the problem, assess the risks and make a concrete recommendation. The report is written in comprehensible language, readable and meaningful for both management and technical staff.
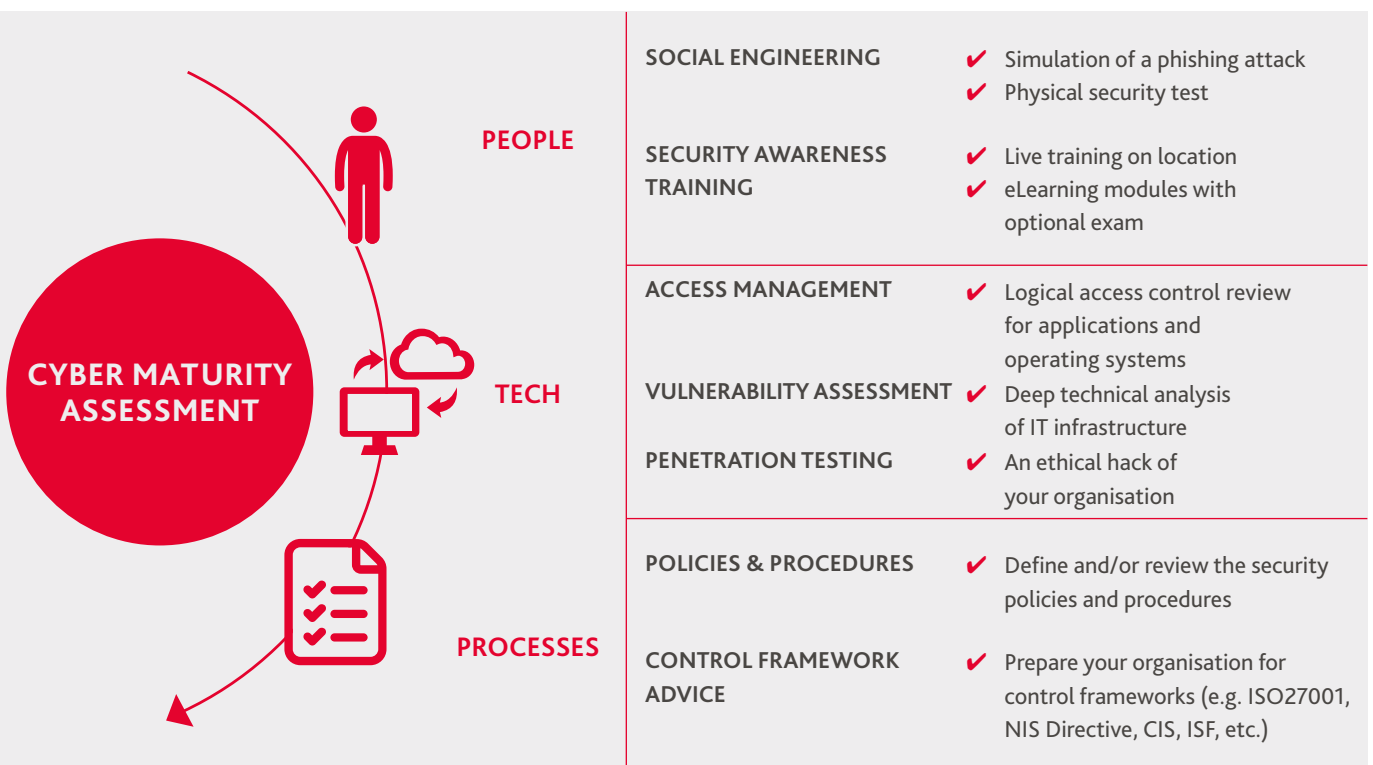
BDO

OUR CYBER SERVICES TAILORED TO YOUR NEEDS

Cyber security is a complex subject, in which many factors and measures come into play. In fact, this is probably one of the reasons why so many organisations are reluctant to take decisive action. Unfortunately, there is no such thing as perfect security, which is why it is important to apply a risk-based approach, focusing first on the highest priorities and risk components. We are happy to help you with that.

As an independent third party, BDO advises organisations to take appropriate cyber measures. As we do not carry out technical implementations ourselves, we are completely independent and our focus is solely on the most pragmatic solution tailored to the organisation.

For each building block, we offer our customers a coordinated and technical approach with clear recommendations and concrete actions to ensure the confidentiality, integrity, availability and security of your data and systems. Our services are delivered by our certified and experienced professionals with the right, proven and effective tools for your entire organisation.

CYBER MATURITY ASSESSMENT

PEOPLE

TECH

PROCESSES

SOCIAL ENGINEERING	✔ Simulation of a phishing attack ✔ Physical security test
SECURITY AWARENESS TRAINING	✔ Live training on location ✔ eLearning modules with optional exam
ACCESS MANAGEMENT	✔ Logical access control review for applications and operating systems
VULNERABILITY ASSESSMENT	✔ Deep technical analysis of IT infrastructure
PENETRATION TESTING	✔ An ethical hack of your organisation
POLICIES & PROCEDURES	✔ Define and/or review the security policies and procedures
CONTROL FRAMEWORK ADVICE	✔ Prepare your organisation for control frameworks (e.g. ISO27001, NIS Directive, CIS, ISF, etc.)

Interested?
Get in touch with:

STEVEN CAUWENBERGHS
Partner Risk Advisory Services

E-mail: steven.cauwenberghs@bdo.be
Tel.: +32 497 05 12 23

FRANCIS OOSTVOGELS
Manager Risk Advisory Services

E-mail: francis.oostvogels@bdo.be
Tel.: +32 474 92 08 00

NICK HUYSMANS
Supervisor Risk Advisory Services

E-mail: nick.huysmans@bdo.be
Tel.: +32 486 31 90 45

▶ Follow us
▶ www.bdo.be

BDO