BDO Advisory



VULNERABILITY ASSESSMENT & PENETRATION TESTING

Improve your cyber resilience

Context

Cyber-attacks and their success rate in network breaches are increasing in frequency and sophistication. At the root of many successful cyber-attacks are the vulnerabilities that exist within network infrastructure, software applications and the very humans that use those networks and applications.

A well-established technique to minimising and mitigating vulnerabilities within network infrastructure and software applications is the use of Vulnerability Assessments and Penetration Testing (VA & PT). The use of VA & PT is a proven and powerful technique to manage the security risk within an organisation or family office.

Further, performing a VA & PT effectively determines your cybersecurity risk profile and general security posture. Understanding and establishing a proven VA & PT process and methodology and utilising the right tools and techniques will ensure the VA & PT accomplishes its goal of improving the overall security of the organisation.



OUR METHODOLOGY TO VULNERABILITY ASSESSMENT

BDO has developed a VA methodology which enables organizations to gain insights from their external IT attack surface and uncover possible weak points that can be exploited by cyber threats. Tool used is a cyber intelligence service that takes an adversarial approach to identify and assess the security posture of the external IT assets of an organization.

Our detailed observations are given a risk classification from High to Low and the definitions of these priorities are given below. The risk classification is being done on a criticality of the vulnerabilities.

OUR APPROACH TO VULNERABILITY ASSESSMENT

BDO will generate a report which will be presented in the form of a dashboard on a web site with one executive management layer and one detailed technical layer. The detailed view will present the list of vulnerabilities detected with the following information:

- Name of the vulnerability as referred in the CVE (Common Vulnerabilities and Exposures) database;
- Detailed description of the vulnerability with potential impact;
- ▶ Criticality of the vulnerability according to the agreed risk scoring methodology:
- ▶ DNS name of the host, with resolved IP address on which the vulnerability is found;
- ▶ The first date on which the scanner detected the vulnerability on the system;
- Mitigation recommendations.





M

High risk indicates that there are serious weaknesses in the security controls and there is a serious risk that must be mitigated as soon as possible.

High



Medium risk indicates that there are weaknesses in the security controls that could lead to a high risk if left unattended and should be mitigated outside normal patching cycles.



Low

Low risk indicates that while there are weaknesses in the security controls these are of limited significance and can be addressed during the normal life cycle management.



OUR METHODOLOGY TO PENETRATION TESTING

BDO developed a methodology used for PT which is based on extensive international experience in delivering similar exercises. The approach is consistent with the best practices in this area and uses, among others, proven elements of the following methodologies and studies:

- OWASP Application Security Verification Standard (ASVS)
- ▶ Penetration Testing Execution Standard (PTES)
- ▶ Open Source Security Testing Methodology Manual (OSSTMM)
- ▶ Open Web Application Security Project (OWASP)
- ▶ NIST 800-42, Guideline on Network Security Testing
- ► Information System Security Assessment Framework (ISSAF)

OUR APPROACH TO PENETRATION TESTING

PT 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. PT is performed in white, black or grey box scenarios.

WHITE BOX I 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 I An attack without prior knowledge of the environment.

GREY BOX I 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.







- 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 recommendation. The
 report is written in
 comprehensible language,
 readable and meaningful for
 both management and technical

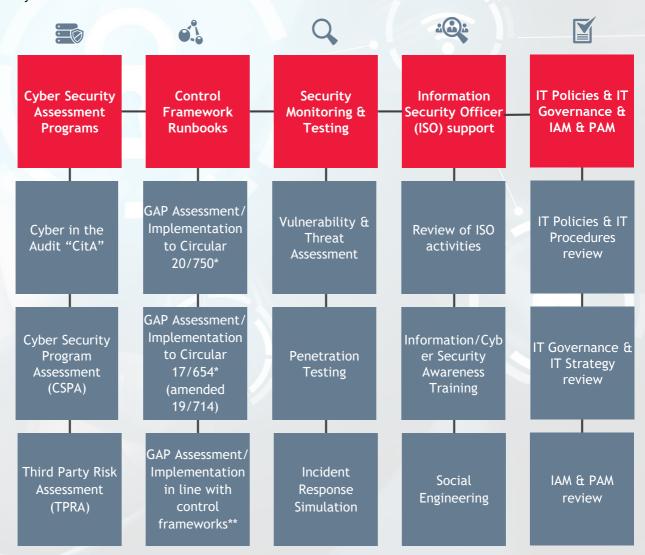


OUR CYBER SERVICES TAILORED TO YOUR NEEDS

At BDO, we believe that cyber-attacks and data breaches are one of the biggest risk facing organizations and their boards today. Impact of cyber incidents could impair an organization's reputation, market value and financial position.

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 organizations to take appropriate cyber measures.

In order to answer to those threats, we offer our customers across all sectors and industries various services for addressing the different weaknesses or regulatory obligations, each with an approach adapted to the size and complexity of our clients. This results in clear recommendations and specific actions to ensure the confidentiality, integrity, availability and security of your data and systems.



- * GAP assessment/Implementation of controls for the financial institutions which are regulated by CSSF in Luxembourg
- * GAP assessment/Implementation of controls to be in line with common control frameworks requirements for compliance with control frameworks (e.g. ISO 27001, ISO 22301, NIST Cybersecurity Framework, etc.)



FOR FURTHER INFORMATION, FEEL FREE TO CONTACT OUR EXPERTS:



Benoît Wtterwulghe **Partner** +352 45 123 795 benoit.wtterwulghe@bdo.lu

Follow us in



www.bdo.lu

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad guidance only.

This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this

publication herein without obtaining specific professional advice.

Please contact the appropriate BDO Member Firm to discuss these matters in the context of your particular circumstances.

Please contact the appropriate BDO Member Firm to discuss these matters in the context or your particular circumstances.

No entity of the BDO network, nor the BDO Member Firms or their partners, employees or agents accept or assume any lability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO is an international network of public accounting firms, the BDO Member Firms, which perform professional services under the name of BDO. Each BDO Member Firm is a member of BDO International Limited, a UK company limited by guarantee that is the governing entity of the international BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BVBA, a limited liability company incorporated in Belgium with its statutory seat

Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BVBA and the member firms of the BDO network is a separate

legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BVBA and/or the member firms of the BDO network. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

© 2021 BDO Advisory. All rights reserved.

