PRUDENCIÁLIS MODELLEZÉSI ÉS IT FELÜGYELETI IGAZGATÓSÁG

Frequently asked questions and answers concerning conducting of vulnerability assessment and penetration test (FAQ)

TRANSLATION

Consultation

1. Is there an opportunity to consult with the Supervision concerning vulnerability assessment and penetration testing?

Yes, there is an opportunity to consult with MNB acting in its supervisory role. A supervised institution can initiate a consultation through its designated institutional supervisor, an unsupervised institution (expert, consultant, etc.) can initiate the same via e-mail address iff@mnb.hu of the IT Supervision Directorate.

Regulation

2. What are the pertinent legal provisions for conducting vulnerability assessments and penetration tests?

The information security requirements for the financial sector are typically regulated by Government Decree 42/2015. (III. 12.) on protecting the information system of financial institutions, insurance undertakings, reinsurance undertakings, investment firms and commodity dealers, and the applicable financial sector laws[1].

Requirements for conducting vulnerability assessment and penetration tests are defined (currently) in Section 13.1.4. points e) and f)[2] of Recommendation 8/2020. (VI.22.) of the Magyar Nemzeti Bank on the protection of information systems (hereinafter Recommendation).

[1] Act CCXXXVII of 2013 on credit institutions and financial enterprises; (henceforth: Hpt.) 67. §, subsection (1), paragraph d), and 67/A. §,
Act CCXXXV of 2013 on certain payment service providers; 12. §, subsection (1), paragraph d), and subsection (3), also 12/A. §,
Act CXXXVIII of 2007 on investment companies and commodity exchange service providers, and on the rules of their activities (henceforth: Bszt.) 12. §,
Based on Act CXX of 2001 on the capital market 318/D. §, Bszt. 12. §,
Act XVI of 2014 on Collective Investment Trusts and Their Managers, and on the Amendment of Financial Regulations; 29. § and 30. §,
Act LXXXII of 1997 on private pension and private pension funds; (henceforth: Mpt.) 77/A. §,
Act XCVI of 1993 on voluntary mutual insurance funds; (henceforth: Öpt.) 40/C. §,
Act LXXXVIII of 2014 on insurance activities; 94. §, subsection (1), paragraph c) and subsections (3)-(6)

[2] 13.1.4. e) vulnerability scanning of systems is performed as follows: in the case of internal and segregated network zones at least annually in accordance with the process specified in the institution's internal rules; in the case of credit card systems, web-based customer service systems, mobile applications, and background systems, scans are conducted at least quarterly; critical errors identified as risks are remediated with no undue delay, non-critical errors are corrected according to a risk-proportionate schedule;

13.1.4. f) penetration testing of applications accessible from the Internet is performed after the correction of errors identified as a risk, prior to go-live, or during any changes impacting security, and then repeated at least annually;

Definitions

3. What is vulnerability testing (vulnerability assessment, vulnerability scan)?

The purpose of a vulnerability assessment is the identification of vulnerabilities in systems, software, or IT environments. One common, more limited method of this is an automated vulnerability scan, where known vulnerabilities in the systems and software are checked with automated tools, then a report is prepared on the identified vulnerabilities and their severity. The sole purpose of a vulnerability assessment is the detection and identification of as many vulnerabilities as possible. The identified vulnerabilities **will not be used** by the tester **for any additional purposes**.

4. What are the types of vulnerability assessments, and which should be applied?

There are several types of techniques to conduct a vulnerability assessment. The Recommendation requires Institutions to conduct a **vulnerability assessment**. The Institution can choose the method of the vulnerability testing, which can either be performed by an automated tool or manually by an expert.
There are two ways to perform an automated vulnerability scan. **Authenticated** scanning is performed when the test is executed with a userID logged into the system (usually with full access permission), or **unauthenticated** scanning occurs when only the externally reachable parameters (ports, services, etc.) are checked.
Section 13.1.4. point e) of the Recommendation **does not specify** the method of the vulnerability assessment to be used. The authenticated scan also covers elements within the system (its extent depends on the set parameters), therefore, much more vulnerabilities can be discovered, but it is necessary to examine its impact on the system before running it. Supplementary tests carried out by experts could be added to the automated ones for the most comprehensive possible result.

5. What is penetration testing?

During penetration testing (ethical hacking) an **authorised** security expert tests the security posture of a system, software, or IT environment with different attack types. The tester attempts to identify and exploit system vulnerabilities. The goal of the penetration test is to determine the potential damage caused **by exploiting known vulnerabilities**, document the processes leading to damage and the protection measures required to prevent them.

6. What are the types of penetration testing, and which should be applied?

We can distinguish “white-box”, “gray-box”, and “black-box” penetration tests. During **“white-box”** testing, the tester **has full access** to all information as well as documentation and in some cases, even the source code of the tested system. This approach provides the widest testing opportunity and the deepest evaluation of the system; however, this is the least realistic simulation of an external attacker’s activities. During **"Black-box"** testing, the tester **does not have any information** about the tested system, acts as an external or internal attacker depending on the access point (internet or intranet). **“Gray-box”** testing means a mix between the previous two modes. Testers **are provided with only certain information** about the system (architecture, operating system description), but they have no direct administrator access.
Section 13.1.4. point f) of Recommendation **does not specify** the method of the penetration test, it shall be determined by the Institution in a risk-proportionate manner, considering the impact of test methods mentioned above.

7. What is Threat Led Penetration Testing (TLPT)?

The TLPT is a sector neutral penetration testing framework that addresses not only technical systems, but also processes (e.g. intrusion detection, incident response). Penetration tests based on TLPT must comply

with the conditions laid down in the framework. For TLPT tests, defining the purpose and method of the specific testing fits closely with the economic sector in which the Institution operates (in this case to the financial sector) as it simulates relevant threats. A TLPT test is always conducted by an independent service provider (Red Team), occasionally leveraging other national or international IT security providers' database and possibly its contribution.

8. What is systems hardening and how can it be verified?

System hardening and secure configuration are a set of **security settings** provided by vendors or independent experts, overriding or supplementing default system parameters. Hardening assessment is often automated, it can be done on its own, but can also be part of a vulnerability assessment. For system hardening and security enhancement configuration see also Section 13.1.4. point g) and specifically Section 8.2.3 (databases) and Section 8.3.2. (virtual environments) of Recommendation.

Compliance

9. In which system environments, on which systems and how often should be the vulnerability test conducted?

According to Section 13.1.4. point e) of the Recommendation, vulnerability assessment should be performed in internal and segregated network zones **at least annually**, in credit card systems, web-based customer service systems, mobile applications, and background systems **at least quarterly**. A regular vulnerability scan must be performed on each system in production environments, and in proportion to the risks in non-production (test, developer, educational) environments. Along with the relevant parts of the Recommendation, other applicable system-specific regulations may be considered as well (e.g. PCI-DSS, SWIFT, CSP). Vulnerability testing is also recommended during the software development phase (see Section 4.4.8. of Recommendation)[3], several times, if necessary, combined with source code review.

10. In which system environments, on which systems and how often should be the penetration test be conducted?

According to Section 13.1.4. point f) of the Recommendation: "penetration testing of applications accessible from the Internet is performed after the correction of errors identified as a risk, **prior to go-live**, or during any changes impacting security, and then repeated **at least annually**;". "Applications accessible from the Internet" means systems, applications and assets (firewall, proxy, gateway) managed by the Institution, which are accessible from the internet, with the addendum that the scanning of external service providers' own systems (service provider's routers, firewalls, applications) and the evaluation and acceptance of test results is also part of the comprehensive vulnerability test. The details of the examination of the latter systems should be set out in a separate agreement with the service providers.

It is recommended to conduct a penetration test also on systems which are not accessible from the internet but process critical data (see Section 4.4.8. of Recommendation)[3].

Practice

[3] 4.4.8. The institution shall ensure that the IT systems, system components and parameters subject to change are tested in a documented manner with reasonable care before go-live. The institution performs functional and non-functional tests, including security tests.

11. How can the negative impact of a penetration test on the production environment be reduced?

Undesirable, unforeseen events can occur during any test. **Increased preparation and impact assessment** are necessary for testing in a production environment. The performance of the penetration test should be subject to an agreement or authorisation between the Institution and the tester based on the Institution's impact assessment, which should include at least the following:

- the systems to be tested;
- the type of penetration test to be conducted;
- the duration of the test;
- the tools to be used for testing;
- the depth of testing (the information and assurance which, after having been obtained, the test should be stopped.).

By providing the above parameters, the Institution may carry out the penetration test best suited to the operation of its live system. In addition, it is advisable to agree on the identity and contact details of an emergency contact available during testing so that if an adverse event occurs, its impact could be minimised.

12. Do testers need to open an account, or become a customer (for example, when testing live internet banking, mobile banking, partner portal, or customer portal)?

One of the purposes of penetration testing is to evaluate whether the customers can use the system only as allowed by the business logic, or beyond their level of authorisation. To perform the test, the tester needs to access **the user interface** in order to detect possible coding flaws, incorrect configuration, and opportunities for abuse (limit bypass, transaction on behalf of others, etc.) by modifying the parameters of the operations that can be performed there. To ensure this, testers may need to open an account, become a customer, or a separate login option must be provided for the tester. In certain cases, testing on a live system is the most effective way, but meeting business conditions and requirements can hinder the completeness of the technical testing. It is within the competence of the Institution to decide, considering the risks, whether the tester should open an account, become a client (performing the testing in a well-defined, pre-agreed, prearranged manner, with special care), or can manage its activities separately in a live system, and whether storing, processing, or deleting test data can interfere with regulatory and other compliance. If the aim of tester's activity cannot be fully achieved in this respect in proportion to the risks, cannot be regulated, or the test data management cannot be implemented in the live system, then the Institution shall act in accordance with Clause 13.

13. What happens if the Institution evaluates that performing a penetration test is too risky on a live system?

Testing on a live system is the most effective way to provide the tester with the opportunity to examine the security of the system from the attacker's point of view. Any other test outside the live system may result in overlooking one or more flaws in the live system. In addition, system connections, data connections, and processes (e.g., for TLPT) can often only be tested on live systems, so some methodologies (e.g. TIBER-EU) also require that tests have to be performed on live systems. If the Institution considers for duly substantiated reasons, that running all or a part of any type of the penetration tests is too risky on the live system, it may perform the testing also **in an environment completely identical to the live system**. In such a case, the Institution shall demonstrate that the environment used for the test is identical to the live environment.

It is considered a good practice to carry out the test just prior to go-live, when no further modifications are expected.

If the deeper penetration tests carried out by the Institution do not take place in the live environment, it could be necessary to compare the system and the runtime environment configurations from the live and

the tested system in a white-box manner, and to retest in proportion to the risks the remmediation of the findings identified in the penetration test, also in a production environment.

14. How to make sure that the test and the production systems are identical in terms of vulnerability assessment?

If the Institution, based on duly substantiated reasons, considers that running any type of the penetration tests – either fully or partially – would be too risky on the live system, then the identicality of the test and the live system environments or the deviation not effecting or obstructing the efficiency and effectiveness of the testing should be demonstrated and documented by verifying the following:

- version control / tracking;
- application configuration, technical parameters in the live and tested environment;
- deployment and testing documentation;
- operational documentation;
- documents of system environments, architecture and interfaces (integration level);
- live and tested environment relevant settings and rules for perimeter protection and network security systems;
- folder permissions (if applicable to the application) in the live and tested environment;
- hardening and vulnerability testing reports for the live and tested environment.

In order to obtain the necessary assurance, the request for and examination of the supporting documents and evidence (e.g. configuration files, certificates, screenshots) is also required.

15. From the anti-money laundering point of view, what rules should be considered if the security testing occurs in a live system?

Expectations concerning anti-money laundering and terrorist financing are set out in the Act LIII of 2017. and its supplement regulations (MNEBDecree No 21/2017., MNB Decree 26/2020.) and further supervisory recommendations. In addition, the MNB has developed a Q&A interface (in Hungarian) and issued other guidance to facilitate uniform legal interpretation.