PROJECT PROCEDURE

MindBytes GmbH

MindBytes GmbH | Probststraße 15 | 70567 Stuttgart
hallo@mind-bytes.de | +49 711 20709567

Management: Christian Stehle, Nina Wagner, Simon Holl
Stuttgart Local Court | HRB 790784 | Tax number 99149/01413
Volksbank Alb eG, IBAN DE04 6309 1300 0513 9800 16

1 Contents

2 Overview

Our projects are divided into the following phases:

1) Preparation: coordination of deadlines, Scoping , kick-off, preparation by client and contractor
2) Implementation & documentation
3) Results: Report & final meeting

3 Preparation

- Determining the **implementation period**
- If the request was submitted via our configurator, a **scoping meeting** follows to present the test object, clarify organizational questions and necessary preparatory steps
- We provide a **checklist** for the preparation

- **Kickoff date** for final preparation and coordination to ensure a smooth start to implementation

3.1 Preparation & input by the client

The client provides all information necessary for the implementation of the project. The information required is discussed during the scoping meeting and provided via a checklist.

3.1.1 For pentests

The following is typically required for pentests:

- **Designation of the test object**, such as the URL of a web application or IP ranges of the infrastructure to be tested
- **Accessibility of the test object**, such as activation for access to protected applications or VPN access to an infrastructure
- **Access to test objects**, such as user accounts for systems or applications with authentication means, such as passwords, certificates and tokens
- Further information, such as documentation or source code of the application, if applicable
- **Exceptions in protection systems**: any protection systems, such as web application firewalls (WAF) and intrusion prevention systems (IPS), are configured for the implementation of the project so that data traffic from the IP address of MindBytes can pass unhindered - if desired, tests can be carried out with connected systems at the end of the project
- **Focus:** Define desired focal points if necessary

3.1.2 For Red Teamings

The following is typically required for Red Teamings:

- **Contact details and availability** of a close circle of insiders ("white team")
- If agreed/requested: **Provision of information** such as domain names, IP address ranges and list of e-mail addresses
- Joint **coordination of the Rules of Engagement** (RoE), i.e. the "rules of the game" in the project
    - Permitted attack surface and methods
    - Attack scenarios and targets
- With Physical Red Teamings
    - Addresses of the destination buildings
    - Signatures for "Get-out-of-Jail" letter for the Red Team (letter of authorization for the Red Team for possible encounters with security services or police)

4 Implementation & documentation

At the beginning of the implementation and after completion of all tests, we send an e-mail for information.

In the event of critical vulnerabilities, an immediate notification is sent.

4.1 In pentests

Depending on the test object, the procedure during the pentest is based on **recognized standards**, such as

- Study "Implementation concept for penetration tests" by the Federal Office for Information Security (BSI)
- OWASP Web Security Testing Guide (WSTG)
- Penetration Testing Execution Standard (PTES)

In pentests, the **execution of the tests is obvious**, i.e. no efforts are made to hide test activities or to remain undetected by any monitoring systems.

The tests are always carried out using **manual methods** supported by **special software** and **automated** state-of-the-art **scans.** The choice of software is highly dependent on the test object and the test environment. The following list is an excerpt of the software used:

- Nessus Professional
- Burp Suite Professional
- Cobalt Strike
- Various open source tools, such as Nmap, Hashcat, Bloodhound and Rubeus

4.2 In Red Teamings

Our approach to red teaming is divided into several phases, which may be repeated when new starting points are reached. Tactics and techniques from the MITRE ATT&CK matrix are used as a basis:

- **Information gathering**: Collecting information about the permitted attack surface, such as systems, breached credentials (access data available on the Internet) and the company itself
- **Defining scenarios**: Designing and, if necessary, coordinating attack scenarios based on the information collected with the client.
- **Prepare scenarios**: Preparing the selected scenarios for implementation

- **Implementation**: Implementing the scenarios

In Red Teamings, **the scenarios** are **carried out covertly**, i.e. the aim is to ensure that test activities remain undetected and do not trigger any alarms in any monitoring systems. If activities remain undetected during the course of the project, the activities carried out may be made more conspicuous in consultation with the client in order to check when activities would be conspicuous.

Throughout the entire project, the Red Team and the people involved on the client side are in **close consultation**.

The tests are always carried out using **manual methods** supported by **special** state-of-the-art **software.** The choice of software is highly dependent on the test object and the test environment. The following list is an excerpt of the software used:

- Burp Suite Professional
- Cobalt Strike
- Various open source tools, such as Nmap, Hashcat, Bloodhound and Rubeus

4.2.1 Important information for the client

- In order to ensure realistic framework conditions for the project, **as few people as possible** on the client side should **be informed about this project**.
- The client **guarantees that the data protection and legal requirements** for this project are met.

5 Results

5.1 Report

The results of the project are provided either in German or English as a PDF report and in tabular form as an Excel file.

5.1.1 For pentests

Our Pentest reports contain:

- A management summary with a risk perspective on the overall picture, the need for action and an overview of the recommended action with priority, estimated time to remedy and costs incurred
- A technical summary with a summary of the results from a technical perspective, presentation of any links between Findings and recommended next steps

- For each Finding a description of the possible security-relevant effects, a classification according to CVSS v3.1 and a recommendation for rectification

5.1.2 For Red Teamings

Our red teaming reports contain:

- A management summary with a risk perspective on the overall picture, the need for action and an overview of the recommended action with priority, estimated time to remedy and costs incurred
- A technical summary with a summary of the results from a technical perspective, presentation of any links between findings and recommended next steps
- A description of the test activities carried out in chronological order
- A description of the client's attack surface as perceived by attackers
- Findings, i.e. security-relevant findings, such as vulnerabilities and weaknesses in monitoring or attack detection behavior
- For each finding, a description of the possible safety-relevant effects, a classification of the risk and a recommendation for remediation
- A list of the Red Team's activities with the associated times (log) so that the customer can trace them and check whether activities have been noticed in their own logs

5.2 Final meeting

As standard, there is an approx. 30-minute final meeting based on the report, in which the results are presented and any questions are answered. Depending on preference, the meeting can take place at the end of the implementation or after the report has been viewed.

If an explicit final presentation has been ordered, the final meeting will be based on a PowerPoint presentation, which will also be provided to the client as a PDF.