TIBER Short Read – A Joint DNB and BuBa Publication

TIBER-EU – A Short Introduction

Introduction

The European financial services sector of the 21st century is characterized by an increasing dependency on interconnected IT systems and third-party suppliers. This interconnectedness presents many opportunities for customers, but also challenges in the field of cybersecurity. Originally, compliance-based assessments were primarily used to address the growing digital risks. Continuous attacks on financial institutions, such as the one by North Korean hackers on the Bangladesh Bank in 2016, have identified the need to complement current efforts with capability-based testing. In order to make the financial services sector more resilient, the TIBER[1] framework has, since its introduction in 2016, been adopted by the ECB Governing Council and implemented in 13 countries, forming a landmark of such capability-based approaches. De Nederlandsche Bank and the Deutsche Bundesbank have produced this short read with the aim to introduce the TIBER-EU framework. This read will explain what TIBER-EU is and how it works.

What is TIBER-EU?

TIBER stands for Threat Intelligence-based Ethical Red-teaming, which is, in short, a framework for the pan-European standardization of red teaming exercises at a very high quality level. Red teaming exercises in turn are a class of cybersecurity tests where entities hire a separate team of ethical hackers (the red team) to try and break into their systems using holistic combinations of different available means such as technical vulnerabilities, human weaknesses (a.k.a. social engineering) as well as physical perimeter security flaws (such as open windows, jumpable turnstiles, etc.). What sets TIBER apart from "ordinary" red teaming is that TIBER uses entity-specific threats to identify the most realistic scenarios an entity might face, based on threat actors' capabilities and intent of attacking this particular entity. Based on this intelligence, real attackers' techniques, tactics and procedures (TTPs) are used by the red team to ultimately improve an entity's own cybersecurity posture. A TIBER test is therefore a very realistic exercise, going way beyond theoretical evaluations of processes and security mechanisms or pen tests.

The goal of TIBER participation is to create a learning experience. There is no such thing as 'passing' or 'failing' a TIBER test. After testing is completed and remediations have been implemented, TIBER participants have the option to (anonymously) share the findings of their test within the trusted community of TIBER participants. Thereby, TIBER participation allows entities to continuously enhance their organisational cyber resilience based on trusted community sharing.

[1] Threat Intelligence-based Ethical Red-teaming

How does TIBER-EU work?

TIBER takes threat intelligence-based red teaming as a very successful tool and turns it into a European standard at a high quality level. This allows big, pan-European entities to test their far-stretched infrastructure in several countries – in only one test. The outcome of this test is then accepted by all jurisdictions that have implemented TIBER. Furthermore, a high quality learning experience is assured by requiring tests to:

- **be conducted on live production systems**. This provides insights into the resilience of an entity in the case of an actual cyber-attack.
- **thoroughly review the critical functions and the underlying systems used by the entity**. The outcomes of this review are used to conduct a resource-efficient red teaming engagement, by focusing on the systems that are crucial for an entity's functioning.
- **conduct a threat intelligence analysis**. This analysis provides insights into an entity's *'crown jewels'*, which are items that threat actors might be after, such as money, information, personal data or critical systems.
- **mimic the skillset of an attacker that has a genuine interest in the entity's crown jewels (intent) and possesses the required skillset (capability) to compromise the targeted systems**. The highly specialised threat actor groups make use of a distinctive combination of TTPs. In a TIBER test external experts emulate a threat actor by using this combination of TTPs. As a result, an entity's defence is tested against those cyber-attacks that pose the largest risk to the entity, making effective use of available resources.
- **involve the board**. Involving the board is important in TIBER-EU, both during and after the test. It ensures the accountability of the test and supports the successful implementation of a remediation plan.
- **include a comprehensive phase for test replay, discussion and learning**. The red teaming engagement in the context of a TIBER-EU test provides many insights, but actions taken after the red teaming phase are just as valuable in order to strengthen the cyber resilience of an entity.

Conclusion and outlook

TIBER-EU is a bespoke European framework for red teaming engagements, which has been adopted by the ECB Governing Council and successfully implemented in 13 countries. The framework first focuses on conducting a threat intelligence-based assessment on an entity. Based on this assessment, systems that underpin critical functions are tested by holistically emulating the TTPs of real, advanced threat actors. Thereby, an entity's cyber defence is tested in a threat-based manner, making efficient use of available resources. A TIBER test is primarily a learning experience, giving an entity insight into the current state of its cyber defence. Besides such learning experience for the entity itself, the anonymous sharing of findings within a trusted community allows for collective improvement of entities' cyber resilience.