6 May 2021

DANMARKS
NATIONALBANK

TIBER-DK in brief

DANMARKS
NATIONALBANK

What is TIBER-DK?

Danmarks Nationalbank and the financial sector have together established the TIBER-DK programme. TIBER stands for Threat Intelligence-based Ethical Red Teaming. In the programme, critical systemic entities perform threat-based red team tests. The purpose is to strengthen cyber resilience and thus promote financial stability.

In brief, TIBER-DK is about learning more about how the individual organisations protect their critical activities from cyberattacks, how they detect that they are being attacked and, last but not least, how they respond to the cyberattack and stop it. Therefore, the objective with TIBER-DK is that the individual organisation learns more about how to protect, detect and respond in order to reduce the risk of the organisation being harmed and of the attack affecting other organisations in the financial sector.

TIBER-DK was launched in collaboration with the Financial Sector Forum for Operational Resilience (FSOR) in December 2018 with the publication of the TIBER-DK framework, which describes how the test is conducted (link). The framework is based on TIBER-EU, which has been developed by the European Central Bank. TIBER-DK was one of the first TIBER programmes in Europe.

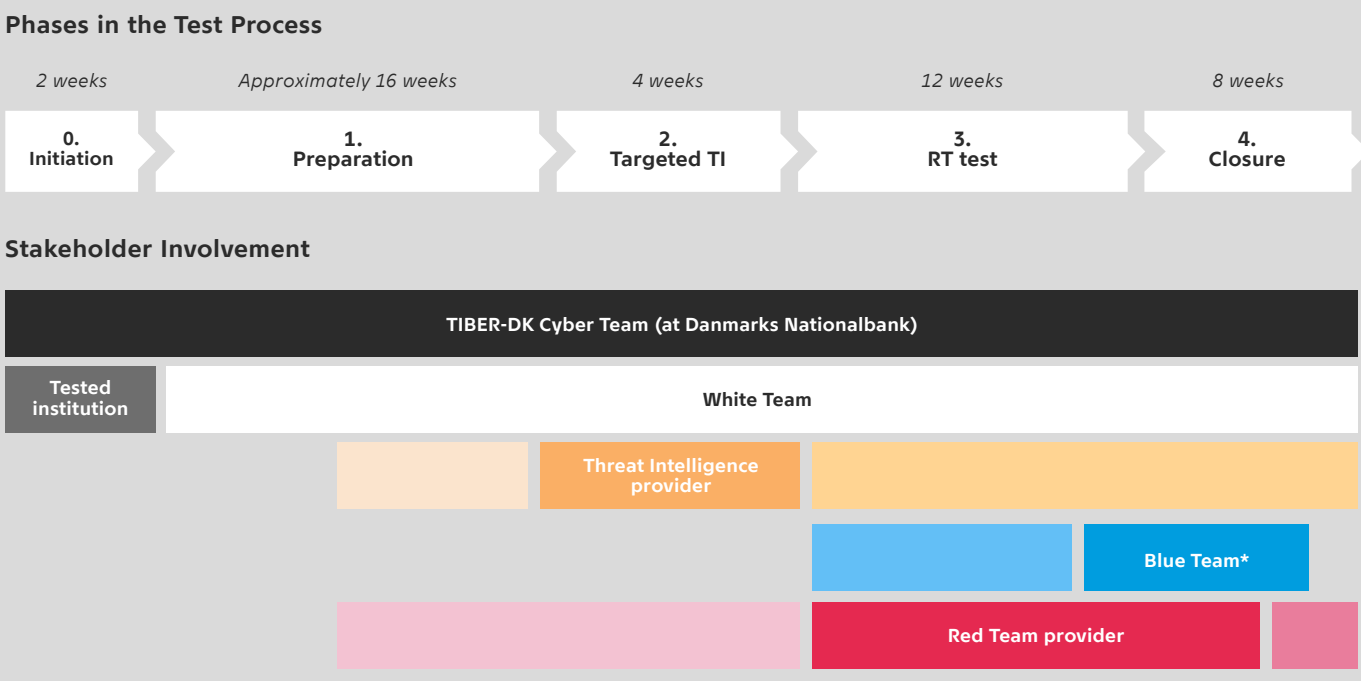
Danmarks Nationalbank is the authority for TIBER-DK, and the test programme is anchored with Per Callesen, Governor of Danmarks Nationalbank. Danmarks Nationalbank's TIBER-DK Cyber Team supports the execution of the tests. The TIBER programme participants are critical systemic entities in the Danish financial infrastructure, which comprises all operative participants in FSOR, including Danmarks Nationalbank itself.

How is the test performed?

TIBER-DK tests have been performed since January 2019. TIBER-DK tests the organisation's cyber defen-

Chart 1

TIBER-DK test process, high-level overview



* The Blue Team at the financial institution is only allowed to know about the test in the Closure phase.

ce and the organisation's response to cyberattacks. The test consists of an attack on the organisation's critical functions, with the objective being to increase cyber resilience where an attack will do the most damage.

The attack itself is conducted by so-called ethical hackers (i.e. a friendly Red Team) imitating sophisticated realistic cyberattacks from organised criminal groups or state-sponsored groups. The ethical hackers use the same tactics, techniques and procedures used by the real advanced hacker groups. This makes the test as realistic as possible.

During the test, the ethical hackers penetrate production systems and networks. There is consequently great focus on confidentiality and risk management to ensure that the test is conducted in a controlled manner without damaging the systems and affecting society.

The TIBER test runs through a number of phases and takes a total of around 10-12 months, with approximately 10 weeks for the actual Red Team attack.

What is the benefit of the test?

The test provides specific learning about potential attacks by real hacker groups and about the measures and improvements that can be implemented to counter them. The learning concerns many areas because the TIBER test covers most cyber defence aspects. It tests systems/networks/technology, processes and roles as well as whether the different security measures are in coherence with each other.

Through the tests, the individual organisation becomes more aware of its own weaknesses and strengths in its cyber defence to the benefit of financial stability.

Learning and experience from individual tests are shared without compromising the individual institutions to increase learning. The most detailed sharing takes place in the so-called sector group for TIBER. Sharing at a more overall level occurs elsewhere, for example in FSOR.

Who are involved in the test?

A TIBER-DK test includes a number of teams in addition to Danmarks Nationalbank's TIBER Cyber Team (TCT).

The White Team (WT) consists of the persons in the tested organisation who know about the test and coordinate it. The WT is kept as small as possible so that the test is not revealed, and the realism of the test is preserved.

The WT procures Threat Intelligence (TI), which examines the threat landscape for the organisation in question. The WT also procures a Red Team (RT), which conducts the actual Red Team attack and consists of the so-called 'ethical hackers'. There are special requirements in the framework for the experience and competences of these suppliers to ensure that they are skilled enough to be able to imitate advanced cyber groups – without harming the critical systems.

The Blue Team (BT) consists of the persons in the organisation in question who are attacked and defend themselves. They have no advance knowledge of the test and act as if it were a real attack.