8. Specific thematic article: Threat-Intelligence-Based Ethical Red Teaming in Belgium (TIBER-BE)

Tijl Jooris

With a high degree of technological progress and growing reliance on related IT infrastructure, cyber risks to the Belgian financial sector are becoming ever more prevalent. One of the NBB's tasks is to monitor Belgian critical market infrastructures and core financial institutions to ensure these key financial entities remain resilient to cyber attacks as to avoid a systemic impact on the Belgian (and by extension European) financial system. To help achieve this goal, the NBB adopted the TIBER-EU Framework in May 2018 and leads implementation of the Threat-Intelligence-Based Ethical Red Teaming framework in Belgium: TIBER-BE.

Since the inception of the TIBER-BE programme, the cyber-threat landscape has changed at a breakneck pace, not least related to geopolitical developments. Besides increased threats from organised criminal groups orchestrating cyber campaigns in pursuit of profit through data theft and ransomware, the Russian invasion of Ukraine has sparked a major uptake in cyber activity by threat actor groups and individuals taking a side in the conflict and conducting operations to support it. For now, related cyber attacks are primarily targeted on Ukrainian and Russian IT infrastructure, but it is not unlikely that stakeholders active in the conflict will eventually shift their focus to targeting nations and entities outside Ukraine and Russia using their newly acquired techniques. This greater threat looming from the East has led Western financial entities and critical infrastructures alike to step up their level of preparedness for potential cyber attacks. In verifying whether a sufficient level of cyber resilience has been achieved and strengthening the defensive measures where needed, the TIBER-BE programme has proven to be a valuable tool. Through the threat-intelligence-based scenarios making up a TIBER-BE engagement, real and relevant threat actors and the techniques they use are emulated. This enables the tested entities to identify and remediate weaknesses that are most likely to be targeted and exploited by these selected threat actors.

After three years of TIBER testing, all entities in the initial scope of the programme have been subjected to a TIBER-BE engagement. While setting up a new initiative like this may be challenging, all tests performed so far can be deemed successful, with a number of lessons learnt for all entities involved. The success of this first cycle helped to establish the framework's reputation and clears the way for subsequent rounds of TIBER-BE testing. The increased credibility brought by the successful first round of TIBER-BE engagements has enabled the programme to grow both in size and thoroughness of the testing approach. For the second round of testing, several new entities have been added to the scope of the programme. This extension has consequently improved the coverage of TIBER testing, further bolstering the programme's ability to enhance the Belgian and European financial system's cyber resilience. Additionally, for those entities that have already completed a TIBER-BE engagement, the experience from the first test has enhanced their familiarity with the TIBER framework which should lead to greater willingness on their part to go through more extensive and more thorough TIBER tests in the future.

BOX 13

Improving implementation of TIBER-BE

Key to improving the TIBER-BE initiative and the willingness of financial entities to be involved in it is the ability to provide feedback and insight as to how to maximise the return on investment of a TIBER-BE test. Feedback helps the NBB to pinpoint areas where the implementation of TIBER-BE can be improved and make adaptations where possible. For this reason, the TIBER-BE programme has singled out a number of ways through which feedback can be shared. This includes (i) a dedicated feedback workshop at the end of TIBER-BE engagements, (ii) a National Implementation Committee where all financial entities falling under the scope of the TIBER-BE programme are invited to share their views on the TIBER framework with the NBB and each other, and (iii) participation of the TIBER-BE team in the TIBER Knowledge Centre, an international committee where all countries that have implemented the TIBER-EU framework come together to exchange insights, best practices and lessons learnt. Feedback obtained through the above-mentioned channels led to the review and rewrite of the TIBER-BE National Implementation Guide, the official TIBER-BE document that was published on the NBB's website in December 2022.