EUROPEAN CENTRAL BANK

EUROSYSTEM

DIRECTORATE GENERAL MARKET INFRASTRUCTURE AND PAYMENTS

ECB-PUBLIC
FINAL

Fourth meeting of Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)

Frankfurt am Main, 16 December 2020

10.30 to 13.00, videoconference

PUBLIC SUMMARY

Participants

- Representatives of the financial infrastructures TARGET Services (TARGET2, Target2Securities), CLS, EBA CLEARING (EURO1, STEP2-T), BI-COMP, STET, EquensWorldline, Iberpay, RPS/EMZ, Euroclear Group, London Stock Exchange Group (Monte Titoli , LCH Clearnet), BME Group (Iberclear), EuroCCP, Mastercard Europe SA, NasdaqClearing, KDPW S.A., Deutsche Börse Group (Eurex Clearing, Clearstream), SWIFT, SIA and Visa Europe.
- Member of the Executive Board of the ECB.
- ECB officials from the Directorate General for Market Infrastructure and Payments.
- Officials from the European Commission, European Banking Authority, ECB Banking Supervision, European Securities & Markets Authority, Deutsche Bundesbank, Banque de France, Banque centrale du Luxembourg, Banco de Espana, Banca d'Italia, Nationale Bank van België, De Nederlandsche Bank, Danmarks Nationalbank, Sveriges Riksbank and Eesti Pank.
- Not attending / excused: EUROPOL, European Union Agency for Cybersecurity (ENISA).

1. Introduction

The Executive Board Member for the ECB and Chair of the ECRB provided introductory remarks. [1]

2. Cyber threat landscape and outlook

A commercial threat intelligence provider provided a presentation on the latest cyber threat landscape and the outlook going forward.

3. Cyber Information & Intelligence Sharing Initiative

The Chair of the ECRB Working Group on information sharing (WG), presented an update on the *Cyber Information and Intelligence Sharing Initiative (CIISI-EU)*. The ECRB members confirm their commitment to support the operationalization of the CIISI-EU building blocks to share vital cybersecurity threat information.

The Chair of the WG informed that public versions of the building blocks of CIISI-EU, namely the Rulebook and Terms of Reference, together with an explanatory ECRB Secretariat paper, have been published on the ECB website under the ECRB heading to offer jurisdictions the necessary tools to build their own information sharing communities.[2]

Overall, there is overwhelming support from both within the EU and internationally for the work conducted by the ECRB members in the realm of information sharing and the CIISI-EU.

The Chair also informed the ECRB on further steps, which would be the full operationalisation of CIISI-EU in the first half of 2021, after which subsequent strategic partnership engagements could be envisaged.

4. TIBER-EU – more than two years of threat lead penetration testing in the EU

The TIBER-EU framework was adopted by the ECB's Governing Council in May 2018.[3] Up to now, ten European countries (i.e. BE, DE, DK, FI, IE, IT, NL, NO, RO, and SE) - and the ECB in its oversight capacity – have adopted the TIBER-EU framework and many tests – at national and at cross-jurisdictional level - have been conducted or are currently ongoing.
The authorities in two jurisdictions were early adopters of the TIBER-EU framework and within their constituencies many entities of their respective core financial infrastructure (banks and FMIs) have tested their cyber resilience. The respective two authorities presented their main

[1] https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html
[2] See www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html
[3] See www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

findings which facilitated an open dialogue among the meeting participants on the learnings of TIBER-EU tests and on the further evolution of threat led penetration testing.

5. DORA – Digital Operational Resilience Act – legislative proposal

On 24 September 2020, the European Commission published its legislative proposal on digital operational resilience for the financial sector, as part of its digital finance package. While the post-crisis changes to the EU financial services legislation put in place a Single Rulebook governing large parts of the financial risks associated with financial services, digital operational resilience was not fully taken up. The DORA legislative proposal is addressing this.
The European Commission gave an overview of DORA, focussing on its relevance and implications for financial market infrastructures with a special emphasis on ICT risk management requirements, ICT incident reporting, operational resilience testing, information sharing arrangements, threat lead penetration testing and the oversight framework on critical ICT third-party service providers. In its presentation, the European Commission stressed the strategic importance of ITC and – more specifically – ITC security for a financial entity and the need for close board level involvement and responsibility.

The ECRB members greatly appreciated the presentation of DORA, the intent of the new regulations and its purpose.

6. Workplan 2021

The ECRB members were invited to reflect on ECRB work priorities for the year 2021, given the limitations the COVID-19 pandemic will continue to impose. The ECRB Secretariat provided the members with an update on progress with the other work items: 1) crisis management and coordination; 2) training and awareness; 3) third party risk; and 4) ecosystem recovery. Due to the extensive attention given to delivering CIISI-EU, progress in the other areas has been limited. The ECRB agreed to kickstart these other work items in 2021, but only after a reflection on the priorities, to be conducted in the first half of 2021.

7. AOB

The next meeting of the ECRB is planned for September 2021, with the final date to be confirmed in due course.