Trust and Technology Blog

By PwC Deutschland | 29.11.2023

EZB Cyber-Stresstest 2024 – Aufgrund zunehmender Cyberangriffe sind Finanzinstitute gefordert, sich mit der eigenen organisationsweiten Widerstandsfähigkeit zu befassen

Auch aufgrund der jüngsten Krisen wie COVID-19,?dem Krieg in der Ukraine sowie den Auseinandersetzungen im Nahen Osten hat die Häufigkeit von Cyberangriffen weltweit zugenommen

– das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt die Cyber-Bedrohungslage aktuell höher ein als je zuvor. Nach Ansicht der EZB könnte ein systemweiter Druck sehr schnell entstehen, wenn u.a. ein Cyberangriff auf eine wichtige (kritische) Infrastruktur erfolgt, weshalb die EZB für 2024 Cyber-Stresstests (als Teil des jährlichen SREP-Prozesses) bei EZB-regulierten Finanzinstituten angekündigt hat. Durch diese soll die Cyber Resilienz bzw. die Widerstands-, Reaktions- und Wiederherstellungsfähigkeit bei Unterbrechung kritischer Dienstleistungen bewertet werden.

Das Szenario für den Stresstest, der für den Zeitraum von Januar bis April 2024 vorgesehen ist, ist ein potenzieller Cyber-Angriff, welcher sich sicher auf die Integrität der Daten des sogenannten Kernbankensystems auswirkt. Die Institute müssen das Kernbankensystem anhand eines durch die EZB bereitgestellten Fragebogens bis Ende November festlegen. Das konkrete Angriffsszenario als solches wird im Januar 2024 durch die EZB veröffentlicht.

Die Methodik zum EZB Cyber-Stresstest sieht ein differenziertes Detaillevel vor. Der durch jedes betroffene Institut anzuwendende Mindestansatz sieht die Befüllung eines Fragebogens als zentrales Ergebnis- bzw. Lieferobjekt, die Meldung des simulierten Cybervorfalls sowie die Nachweisbarkeit der Reaktionsfähigkeit im Rahmen der bestehenden durch das Institut schriftlich-fixierten-Verfahren vor. Etwa 20 Institute, die nach verschiedenen Kriterien durch die EZB bestimmt werden, sind im Rahmen eines Deep-Dive Ansatzes darüber hinaus dazu verpflichtet, einen umfassenden IT-Recovery Test im Hinblick auf ein Kernbankensystem durchzuführen. Zudem behält sich die EZB vor, im Rahmen einer möglichen Onsite Inspection die Ergebnisse zu validieren.

Die aktuelle Vorbereitung der Cyber-Stresstests in diversen Projekten zeigt auf, mit welchen vielschichtigen Fragestellungen sich Institute befassen müssen, um für den „Ernstfall“ bestmöglich gewappnet zu sein. Neben der Analyse und Definition des eigentlichen Kernbankensystems, der Ableitung/Bewertung quantitativer Schäden und der zeitlichen Erkennung eines Angriffs werden ebenso Fragestellungen diskutiert, die für viele Institute nicht alltäglich sind – z.B. Umfang mit einer bestehenden Cyber-Versicherung, Lösegeldbeschaffung/-bezahlung per Bitcoin oder Krisenkommunikation Richtung Kunden.

Auch wenn der Cyber-Stresstest nur für einen Teil der Finanzinstitute relevant ist, lässt sich festhalten, dass eine inhaltliche Auseinandersetzung mit dem Vorgehen bzw. den Angriffsszenarien sowie den erforderlichen BCM-/ITSCM-Maßnahmen (u.a. Response- und Recovery-Pläne) grundsätzlich dringend anzuraten ist, um die Reaktionsfähigkeit der Organisation für spezifische Cyber-Angriffsszenarien sicherzustellen.

Keywords

Coronavirus (COVID-19), IT-Sicherheit, Russland-Ukraine-Krieg, Stresstest

Contact

Karsten Wilop

Düsseldorf

karsten.wilop@pwc.com