EUROPEAN CENTRAL BANK

EUROSYSTEM

Andreas Erl

Principal Expert

Directorate General
Market Infrastructure and Payments

Strategy for reducing the risk of wholesale payments fraud related to endpoint security

AMI-Pay

Frankfurt, 19 November 2018

Overview

Overview

Background

- To address the evolving threat landscape the CPMI published its report on Reducing wholesale payments fraud related to endpoint security in May 2018
- The key objectives of the report are to
  - Encourage and help focus industry efforts aimed at reducing the risk of wholesale payments fraud
  - Promote the clarity, comprehensiveness and effectiveness of industry efforts by providing an analytical approach and common terminology
  - Support industry dialogue aimed at exploring potential common issues and opportunities to coordinate on approaches and practices to reduce the risk of wholesale payments fraud
- The strategy is designed to be taken into account by all relevant public and private sector stakeholders in reducing the risk of wholesale payments fraud

Endpoints in the wholesale payment ecosystem I/II

- Endpoint: a point in place and time at which payment instruction information is exchanged between two parties in the ecosystem, such as between:
  - a messaging network and a participant in the network
  - a payment system and a participant in the system
  - a payment system and a messaging network
- Endpoint does not relate solely to parties at either end of a payment transaction chain, but rather participants of wholesale payment systems or messaging networks that can transmit and receive payment instructions on behalf of themselves or others
- Endpoint security is built upon measures taken with respect to endpoint hardware, software, physical access, logical access, organisation and processes

Seven elements of the strategy

- Seven elements of the strategy
  1. Identify and understand the range of risks
  2. Establish endpoint requirements
  3. Promote adherence
  4. Provide and use information and tools to improve prevention and detection
  5. Respond timely to potential fraud
  6. Support ongoing education, awareness, and information sharing
  7. Learn, evolve, and coordinate
- Need for flexibility
- Each participant or “endpoint” has incentives to prevent fraud
  - Financial loss and reputational risk
- Endpoint security is ultimately the responsibility of the endpoint

Overview

Endpoint security in TARGET2

- Core principles for Systemically Important Payment Systems, January 2001
  - Core Principle VII:
    - security of any system is only *"as strong as its weakest link";*
    - Operational reliability depends on all components, including for example telecommunications network;
    - concern of the operator *"…can go beyond the participants' initial interface with the system, to include any of the participants' operations which could adversely impact the payment system."*
- PFMI, April 2012
  - Principle 17:
    - Participants: *"To manage the operational risks with its participants, an FMI should consider establishing minimum operational requirements for its participants. For example, an FMI may want to define operational and business continuity requirements for participants in accordance with the participant's role and importance to the system."*
    - Addresses also third party service providers

Measures in place to support endpoint security

- TARGET2 offers a set of tools to support endpoint security
  1. TARGET2 self-certification arrangement
  2. Incident reporting
  3. SWIFT Customer Security Programme
  4. Business transaction pattern monitoring and alert mechanism

TARGET2 self-certification

- In place since the go-live of TARGET2 in 2007
- Legal basis: TARGET2 Guideline (Art. 28.3, Annex II)
- TARGET2 users self-certify compliance with certain requirements set-up by the Eurosystem in its capacity as TARGET2 operator
- Requirements based on internationally recognised standards
- Signed self-certificate confirming compliance
- Action plan
- TARGET2 self-certification arrangement is reviewed at regular intervals

Incident reporting

- Users are requested to report incidents affecting Confidentiality, Integrity, Availability of their internal systems to the central bank with which they have established a contractual relationship
- Thresholds (incident affecting availability)
  - critical participants: 30 minutes of unavailability
  - Non-critical participants: no quantitative figure; impact on the smooth functioning of TARGET2 or other users
- Incidents affecting Confidentiality and/or Integrity: trust based
- Information obtained can be used for learning purposes

SWIFT Customer Security Programme

- TARGET2 is predominantly SWIFT based
- SWIFT introduced the SWIFT Customer Security Programme (CSP)
- SWIFT users
  - are required to self-attest compliance against mandatory security controls
  - have the possibility to request compliance information from other SWIFT users
- Online portal: the “Know Your Customer” Registry Security Attestation Application (KYC-SA portal)
- Central banks monitor the compliance level of TARGET2 users connected via SWIFT
- Full compliance with the SWIFT CSP mandatory controls is expected by the end of 2018

Business transaction pattern monitoring and alert mechanism

- Basic concept: deviations from normal transaction patterns could potentially indicate a fraudulent transaction
- tool triggering alerts if deviations from usual patterns are observed
- validity of the alerts to be verified by the operational staff in cooperation with customer
- Implementation in progress
- Main aspects
  - no fraud case in TARGET2: difficulty to assess validity of the designed tool
  - ex-post: does not aim at preventing, unless a recurrent daily event
  - focus on customer payments (SWIFT MT103)
  - granularity: bank, day
  - patterns based on a reference period of 2 years, rolling window
  - deviations from patterns (i.e. exceeding the mean plus 3 to 4 standard deviations)

Overview

Endpoint security in TARGET2 – Future changes

- TARGET2 operator conducted a self-assessment suggesting a high level of compliance with the CPMI strategy
- Current arrangements can be strengthened further
  - Indirect participants currently outside the scope of existing arrangements
  - Participants shall be encouraged to carry out intraday reconciliations of the TARGET2 accounts
- Challenges
  - Future TARGET services will become network agnostic
  - Enhancement of the tool to ex-post detect cases of fraud (e.g. more sophisticated indicators, refinement of the methodology, machine learning)

Thank you for your attention