Estrategia para reducir el riesgo de fraude en los sistemas de grandes pagos relacionado con los puntos de acceso.

AMI-Pay España. Grupo nacional para infraestructuras de pago

Madrid
14 de noviembre de 2018

DEPARTAMENTO DE SISTEMAS DE PAGO

Reducción del riesgo de fraude en los sistemas de grandes pagos – Informe CPMI

Fraude: Amenaza real

2016 – Robo al Banco Nacional de Bangladesh

EL ECONOMISTA

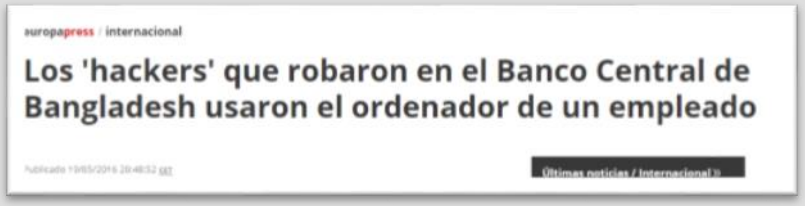
Bangladesh pierde 100 mdd en supuesto ciberataque

El banco central de Bangladesh trabaja para recuperar unos 100 millones de [illegible] supuestamente robados por hackers chinos de una cuenta en el Federal Reser[illegible] York.

AP
09 de marzo de 2016, 07:12

Ciberatraco multimillonario al sistema de la Reserva Federal de los EE.UU.

• Los piratas informáticos realizaron transferencias bancarias por valor de 100 millones de dólares desde la cuenta de la Fed del Banco Central de Bangladesh a países asiáticos



europapress / internacional

Los 'hackers' que robaron en el Banco Central de Bangladesh usaron el ordenador de un empleado

Publicado 19/03/2016 20:48:52 GMT

Últimas noticias / Internacional

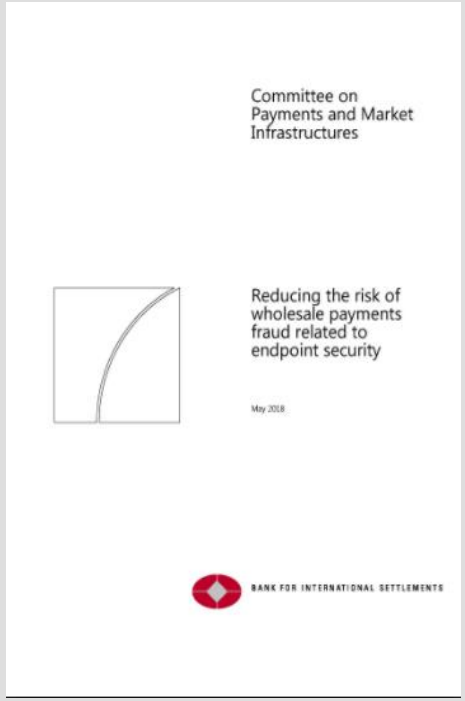
Robo cibernético a banco de Bangladesh

También durante 2016, cibercriminales un robaron 81 millones de dólares a un banco de Bangladesh mediante el uso de un código malicioso detectado por ESET como una variante de Win32/Agent.XZH. Se trata de un código altamente complejo que presenta una funcionalidad sofisticada y que permitió a los cibercriminales acceder al software de mensajería utilizado por más de 11.000 bancos e instituciones financieras de más de 200 países conocido como SWIFT Alliance Access.

¿ Cómo actuar?

- ✓ **Ecosistema complejo** – Interconexiones sistemas grandes pago (vía mensajería) con
  - Bancos
  - Infraestructuras
  - Otras entidades financieras
  - Proveedores de servicios tecnológicos
- ✓ **Énfasis en la seguridad de los puntos de entrada (*endpoint*)**

"Reducing the risk of wholesale payments fraud related to endpoint security" (CPMI, 2018)



Reducción del riesgo de fraude en los sistemas de grandes pagos – Informe CPMI

- **Puntos de entrada: Puntos de intercambio de información de pago entre dos partes del ecosistema** (e.j.: sistema de pago y red mensajería; sistema con un participante, red de mensajería con participante)**.**

✓ Medidas de seguridad **(Amplio espectro)**

- Hardware
- Software
- Acceso físico
- Acceso lógico
- Organización y procesos

- **Debilidad en un punto entrada – Repercusión resto ecosistema**

ESTRATEGIA CPMI: Enfoque holístico

Reducción del riesgo de fraude en los sistemas de grandes pagos – Informe CPMI

ESTRATEGIA: 7 LÍNEAS DE ACTUACIÓN

1. Identificar y entender los diversos tipos de riesgos.
2. Establecer requisitos de seguridad (prevención, detección, respuesta, comunicación con el resto de la red) en los puntos de acceso.
3. Promover (los operadores y los participantes) la adherencia a los requisitos anteriores de sus respectivos puntos de acceso.
4. Facilitar y utilizar información y mecanismos que ayuden a mejorar los sistemas de prevención y detección de fraude.
5. Responder a tiempo al fraude potencial.
6. Promover la educación continua y compartir información.
7. Actitud proactiva (ej.: realizar un aprendizaje continuo, adoptar medidas y actuar activa y coordinadamente con los otros participantes).

ESTRATEGIA COMPLEMENTARIA:

- **CPMI-IOSCO PFMI**
  &
- **CPMI-IOSCO Guía de ciberresiliancia FMI**

¿ Cómo implementarla?

- ✓ Compromiso todos los actores
- ✓ Flexibilidad (especificidades cada sistema y jurisdicción)
- ✓ Coordinación y armonización actuaciones
- ✓ Reparto claro tareas y responsabilidades
- ✓ Establecimiento calendario de actuación

Bancos centrales y CPMI: CATALIZADORES de la estrategia

(Seguimiento 2018 & 2019 (e.j.: cuestionario))

IMPORTANCIA IMPLICACIÓN TODOS LOS BANCOS CENTRALES

IMPLEMENTACIÓN DE LA ESTRATEGIA POR EL EUROSISTEMA :

- **Identificación actores relevantes**
  - ✓ Sistemas de grandes pagos: **TARGET2 y EURO1** (clasificados como Sistemas de pago de importancia sistémica)
  - ✓ Proveedores de servicios de mensajería: **SWIFT** (supervisado por el G10)
    - ✓ *Vigilantes*: ***BCE*** *(vigilante principal de TARGET2 y EURO1) &* ***Banco Central de Bélgica*** *(vigilante principal de SWIFT)*
  - ✓ Participantes en los sistemas:
    - ✓ ***Entidades financieras:*** *Mecanismo Único de Supervisión (**SSM**)*
    - ✓ ***Sistemas vinculados***

Reducción del riesgo de fraude en los sistemas de grandes pagos – Informe CPMI

- **Operador:** Implementación estrategia por su sistema de grandes pagos: TARGET2
- **Vigilante:** Valoración actuaciones realizadas por parte de TARGET2 y EURO1
- **Catalizador:** Fomento, coordinación y seguimiento de las actuaciones conjunto actores relevantes

GRACIAS POR SU ATENCIÓN

BANCO DE ESPAÑA
Eurosistema

DEPARTAMENTO DE SISTEMAS DE PAGO