Koninkrijk seminar 2016

Lisette Buckley
Senior Policy Advisor Integrity Supervision

Konikrijk seminar 2016

- Integriteit in de financiële sector
- Integere uitoefening van het bedrijf
- Richtlijn Integere Bedrijfsvoering

Wat *wordt verstaan onder incident ?,* ***Waarom*** *is het zo belangrijk ? en* ***Hoe*** *moet worden omgegaan met een incident ?*

Definitie van incident:

Een gedraging of gebeurtenis die een ernstig gevaar vormt voor een integere uitoefening van het bedrijf van de desbetreffende instelling.

- **Gedraging kan bestaan uit een doen of nalaten van:**
  - **a. personeelsleden;**
  - **b. bestuurders;**
  - **c. leden van de raad van commissarissen en raad van toezicht;**
  - **d. derde (natuurlijke of rechtspersoon) die werkzaamheden verricht ten behoeve van de instelling.**

- **Gedragingen en gebeurtenissen die hebben geleid of naar verwachting zouden kunnen leiden tot:**
  - **a. aangifte bij de justitiële autoriteiten;**
  - **b. potentiële bedreiging voor het voortbestaan van de instelling;**
  - **c. ernstige tekortkoming in de opzet of werking van de procedures en maatregelen voor een integere bedrijfsvoering;**
  - **d. ernstige mate van publiciteit, financiële gevolgen of reputatieschade van de instelling.**

Richtlijn:

1. Een instelling beschikt over procedures en maatregelen met betrekking tot de omgang met en de vastlegging van incidenten en legt deze schriftelijk vast.

   Die procedures en maatregelen voorzien in elk geval in:

   a. een degelijke administratieve vastlegging van:
      - de kenmerken van het incident;
      - de gegevens over de personen die het incident hebben veroorzaakt of anderszins daarbij betrokken waren; en
      - de naar aanleiding van het incident genomen maatregelen.

   b. de wijze van afhandeling van incidenten; en

   c. de informatieverstrekking aan de CBA.

2. Een instelling neemt naar aanleiding van een incident maatregelen die gericht zijn op het beheersen van de opgetreden risico's en het voorkomen van herhaling.

3. Een instelling informeert de CBA onverwijld schriftelijk.

Konikrijk seminar 2016

Voorbeelden van incidenten zijn onder meer:

- **(interne of externe) fraude;**
- **inval door strafrechtelijke autoriteiten (huiszoekin**
- **onderzoek ter plaatse door de Servicio di Impuesto;**
- **rechtszaken die gevolgen met zich kunnen brengen voor de financiële positie en/of reputatie van de instelling dan wel de sector;**
- **(tijdelijk) niet of onvoldoende functioneren van het IT systeem; en**
- **achterstand in het melden van ongebruikelijke transacties.**

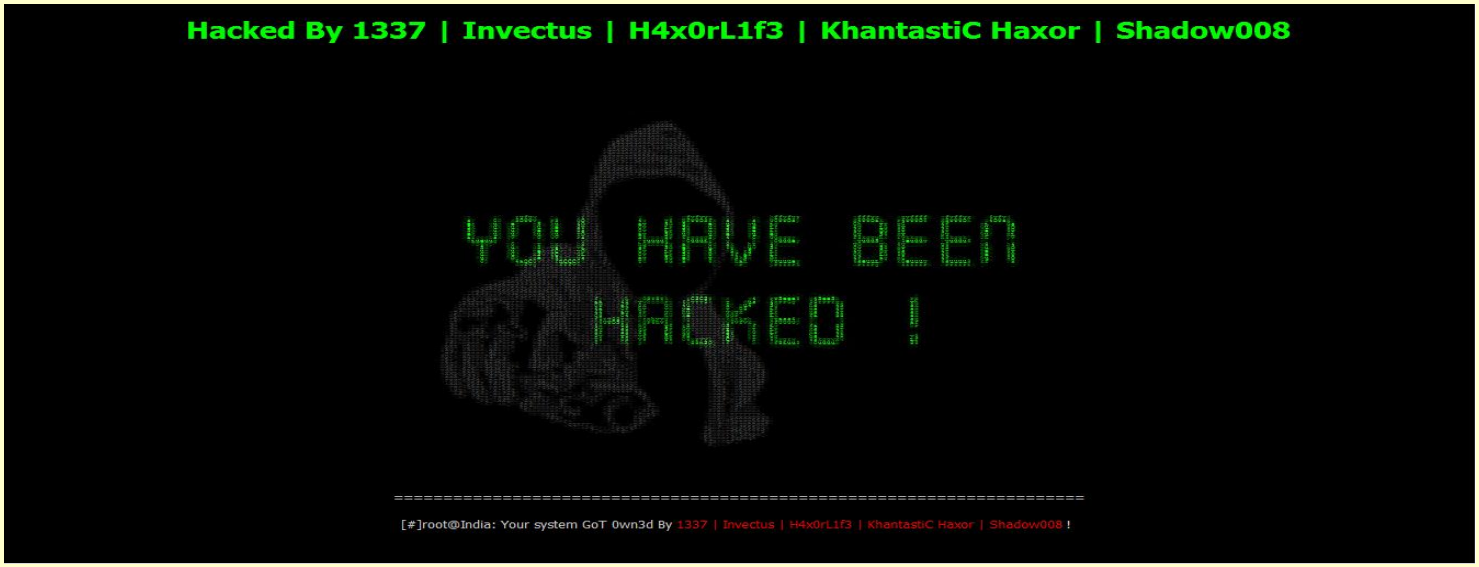
- Over 11,000 financial institutions worldwide use the SWIFT system to move funds internationally
- Ecuadorian bank lost $9M in January 2015
- Vietnamese Tien Phong bank attacked in December 2015
  - Intercepted an attempt to remove $1.1M using an outside vendor's infrastructure.
- Bangladesh central bank, $81M stolen February 2016
- October 2015 attack on a bank in the Philippines also rumored
- Symantec has publicly linked SWIFT attacks to the 2014 SONY attack, (malefactors nicknamed "Lazarus") and hence the North Koreans.

SWIFT

SUDDENLY, A CENTRAL CONCERN: THE "SWIFT" INCIDENTS

(c) 20156Tellagraff LLC

Konikrijk seminar 2016



Konikrijk seminar 2016

De interne organisatie van een instelling dient zodanig te zijn opgezet, dat:

- **incidenten worden geconstateerd;**
- **incidenten worden vastgelegd; en**
- **incidenten aanleiding zijn tot het nemen van correctieve maatregelen.**

Naast maatregelen tegen de veroorzaker zal de instelling ook maatregelen moeten nemen bestaande uit:

- **het verbeteren van interne procedures;**
- **het aanpassen van het beleid ter preventie van herhaling van een vergelijkbaar incident; en**
- **beheersing van het aan het incident onderliggende risico.**

Konikrijk seminar 2016

Konikrijk seminar 2016

Een instelling informeert de CBA onverwijld omtrent incidenten:

- **zo spoedig mogelijk;**
- **uiterlijk binnen 2 werkdagen (48 uren) nadat het incident is gedetecteerd.**

Een mondeling bericht over een incident moet altijd schriftelijk worden bevestigd binnen 2 werkdagen (48 uren).

Wat moet er gemeld worden aan de CBA ?

- het incident;
- of er onderzoek is verricht;
- wat voor soort onderzoek en door wie;
- feitelijke bevindingen van het onderzoek;
- kwalificatie van het incident;
- zijn er maatregelen getroffen en wat voor soort maatregelen;
- wat zijn de gevolgen van het incident;
- heeft de insteling of de sector schade geleden;
- is het risico geïdentificeerd in de risico-analyse van de instelling;
- was het risico voldoende gemitigeerd in het beleid en de procedures;
- zijn de procedures en maatregelen correct geïmplementeerd;
- dient het beleid en de procedures bijgesteld te worden ter voorkoming van herhaling;

Konikrijk seminar 2016

Een ontvangen incidentmelding wordt door de CBA op de volgende punten beoordeeld:

- **is de verstrekte informatie volledig;**
- **hoe ingrijpend is het incident (sense of urgency);**
- **heeft de instelling zelf maatregelen genomen en zo ja welke;**
- **zal er een (forensisch) onderzoek naar het incident door een onafhankelijke deskundige worden verricht;**
- **dient de naleving door de instelling van de RIB door een onafhankelijke derde te worden onderzocht.**

De CBA kan aan de instelling een aanwijzing geven met een instructie tot het verrichten van een (onafhankelijk) onderzoek met terugkoppeling aan de CBA van het resultaat. Ook kan de CBA zelf een onderzoek bij de instelling verrichten ter beoordeling van de naleving van de RIB of enige bepaling van de toezichtwet- en/of regelgeving.

Ingeval van vaststelling van overtreding van de RIB of enig andere toezichtwet- en/of regelgeving, kan de CBA overwegen tot oplegging van informele of formele maatregelen.

Praktijkvoorbeelden van incidenten:

- **vermeende fraude/corruptie door een directielid (bevoordeling van derden);**
- **IT hacks;**
- **het verstrekken van reference letters door onbevoegde werknemers;**
- **het onder invloed van alcohol veroorzaken van een verkeersongeluk en daarna doorrijden door een medewerker met een integriteitsgevoelige functie;**
- **interne fraude middels electronische overmaking van gelden op de bankrekening van een instelling naar privé rekening;**
- **fraude door een werknemer met cheques door het vervalsen van de handtekening van de tekeningsbevoegde**

Konikrijk seminar 2016