Lessons learnt for CERT-s?

Deloitte.

FUNDACJA
bezpieczna
cyberprzestrzeń

RCB
Rządowe Centrum
Bezpieczeństwa

The „CYBER EXERCISES” trend

- European and worldwide trend in organising „Cyber Exercises”
  - Cyber Europe 2010/2012/2014 / ENISA
  - Cyber-Storm / US
  - Waking Shark 2 / UK

- A continuation of the cycle which started in 2012
- Cyber-EXE Poland 2012 was dadicated for the CIIP sector

CYBER-EXE POLSKA 2012

Cyber-EXE Polska 2012 – CIIP sector

Two editions of the Cyber-EXE Polska exercises

- Cyber-EXE Polska 2012:
  - Gaz-System SA / PSE Operator
  - Government Centre for Security
  - Ministry of Defense / Police
  - Military University of Technology / Wroclaw University of Technology
  - CERT Orange Poland
- Cyber-EXE Polska 2013: banking sector in Poland
  - Commercial banks (from top10)
  - Anonymous participation based on the banks' decision (same like in Cyber Europe 2012)

CYBER-EXE POLSKA 2013

Organiser

- CYBERSECURITY FOUNDATION

cybersecurity FOUNDATION

Organising Partners

- DELOITTE POLAND
- POLISH GOVERNMENT CENTRE FOR SECURITY

Deloitte.

RCB Rządowe Centrum Bezpieczeństwa

Supporting Partners

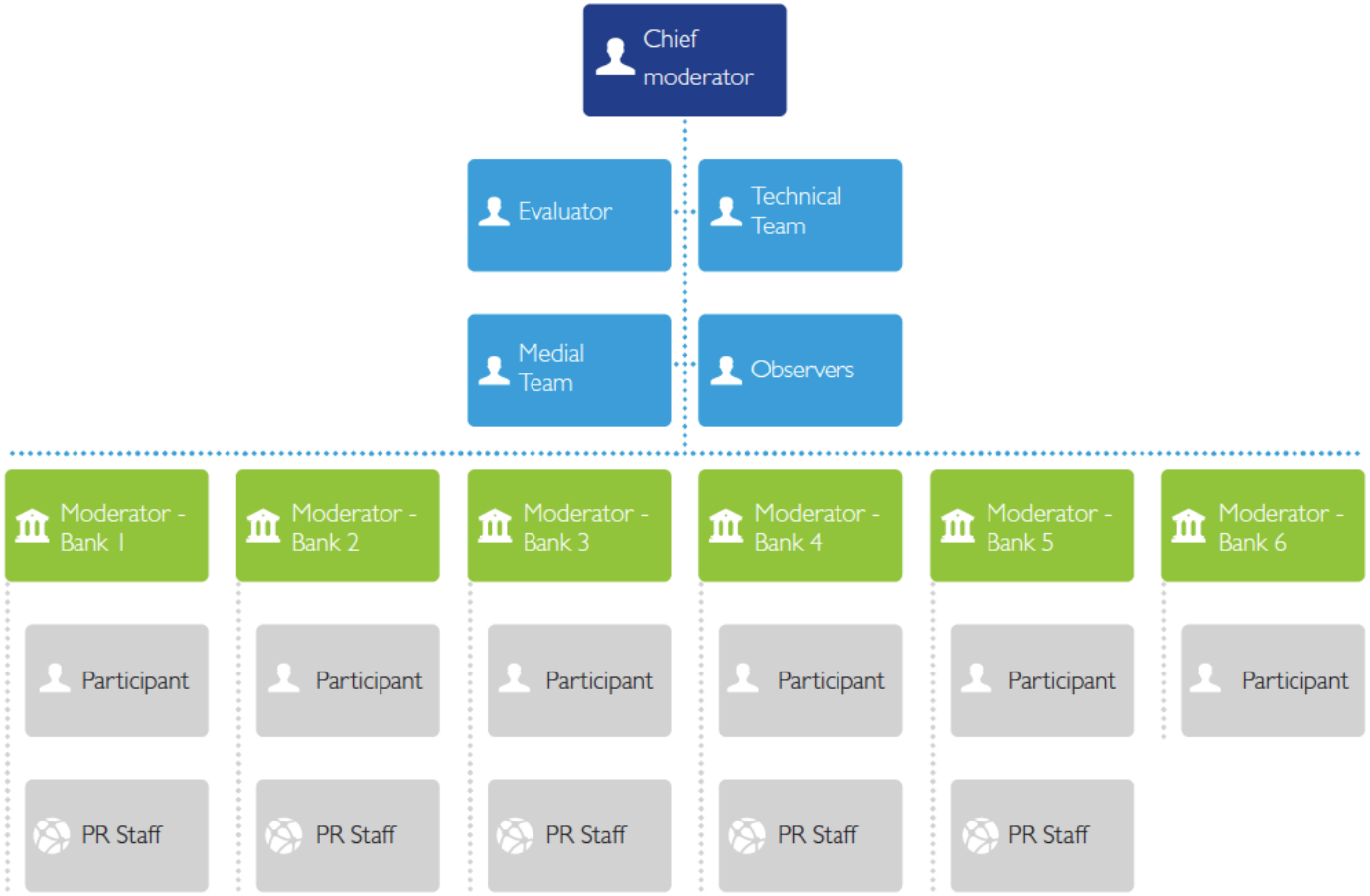
- MINISTRY OF FINANCE
- NATIONAL BANK OF POLAND
- POLISH FINANCIAL SUPERVISORY AUTHORITY
- POLISH BANKS ASSOCIATION

Ministerstwo Finansów

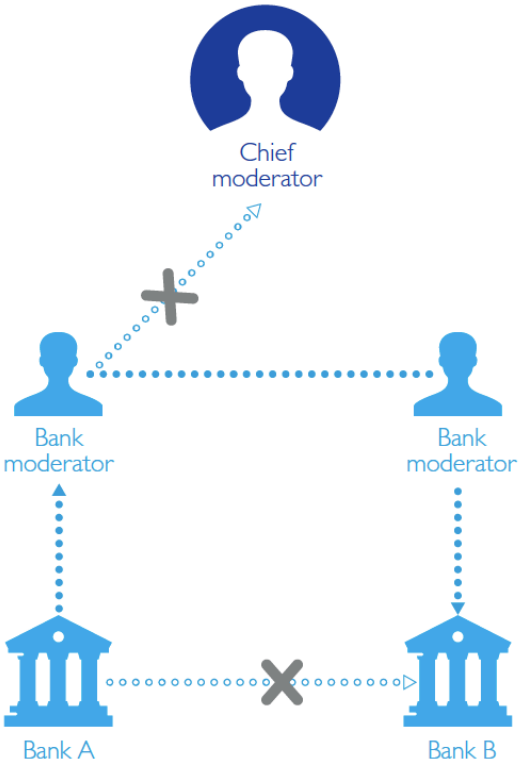
NBP Narodowy Bank Polski

Komisja Nadzoru Finansowego

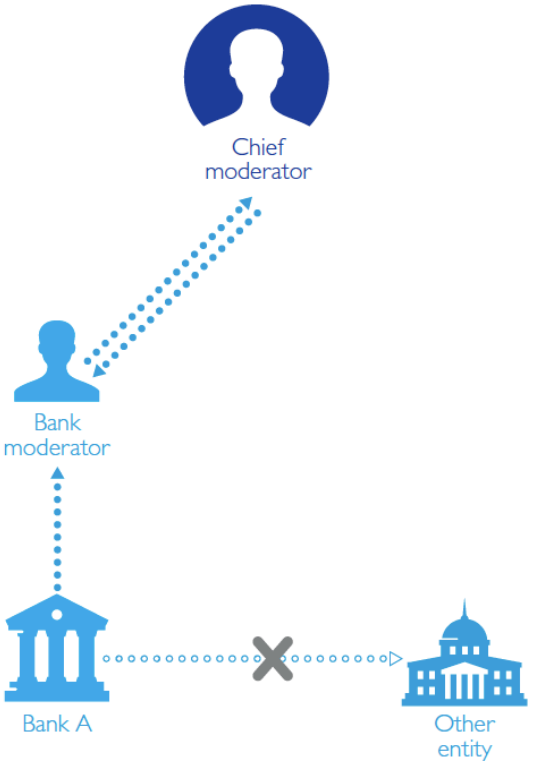
Organisational structure



BANK TO BANK



BANK TO OTHERS

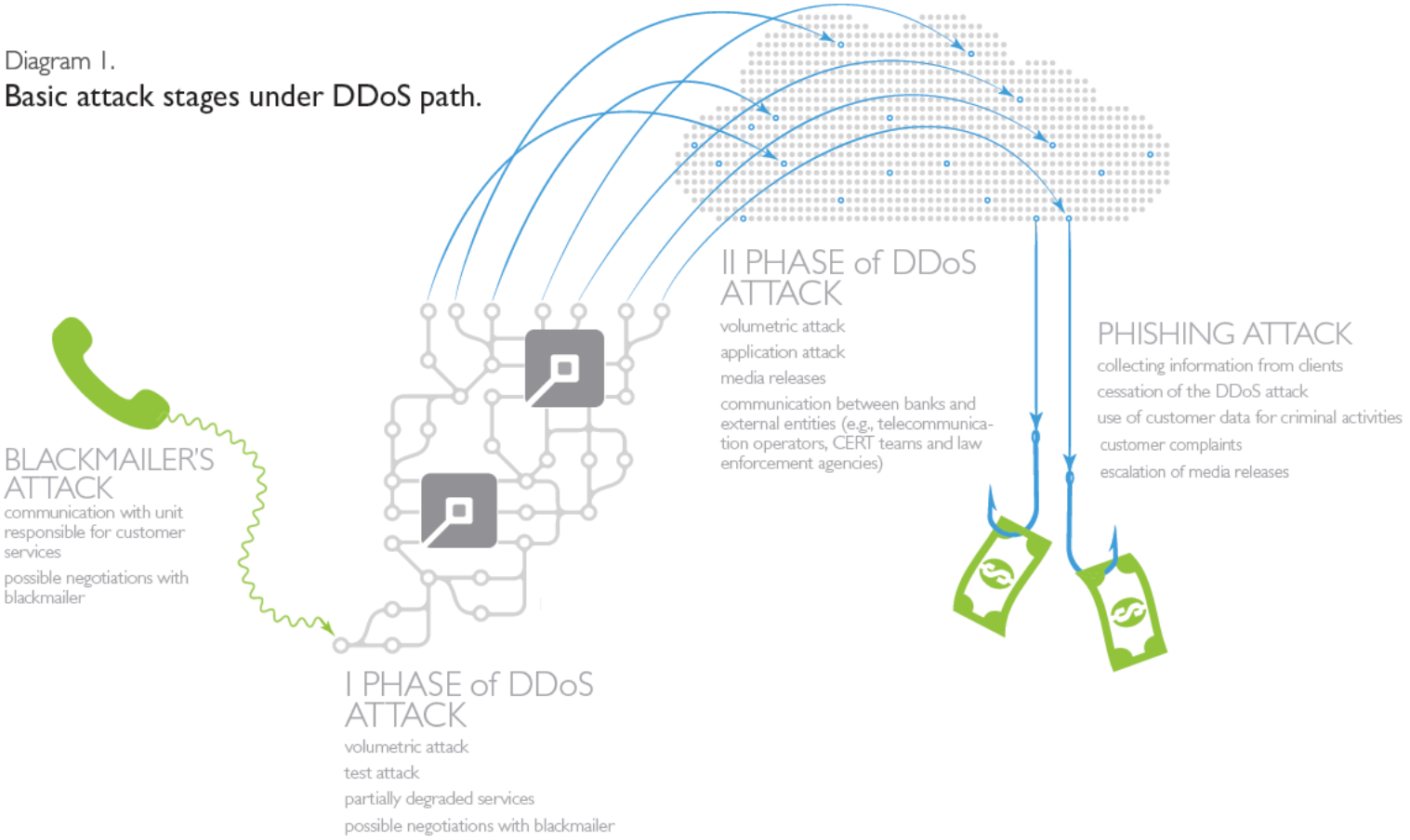


The exercises objectives

- Checking the organisations' cyber attack emergency repsonse procedures
- Identification of interdependencies among banks, regulators and othere entities whithin the financial sector
- Checking communication among banks, regulators and other entites whitin the financial marketwego

DDoS ATTACK SCENARIO

Diagram 1.
Basic attack stages under DDoS path.



APT ATTACK SCENARIO

PUBLICATION OF CONFIDENTIAL INFORMATION

press release

residual confidential information

blackmail and possible negotiations

ATACK ANALYSIS

collecting as much information about the source of the attack as possible

escalation of media releass

blackmail and possible negotiations

LIAISON WITH EXTERNAL ENTITIES

cooperation among the banks

possible joint ventures undertaken by banks

cooperation with external entities (e.g., CERT teams and law enforcement agencies)

Conclusions and recommendations

- For implementing whitin banks
  - Organisational
  - Related to an external communication
- Fro implementing in the whole sector

CYBER-EXE POLSKA 2013

Conclusions and recommendations for BANKS

Conclusions:

- To know procedures is not enough
- There is a big dependency on external partners and organisations
  - Telecoms
  - LEAs, CERTs

Recommendations:

- Aquiring up-to-date knowladge
- Basic trainings for all bank employees
- Advanced security training for key personnel
- Building relationships and cooperation during „peace” (Si vis pacem para bellum)
- Improving skills regarding blackmailing negotiations

Conclusions in regards to external communication

CYBER-EXE POLSKA 2013

Conclusions:

- Prompt reaction to public news and customers' „publications"
- Good coordintation between internal PR team and crisis management unit
- Dalayed reaction to „individual approach by jurnalists – („talking points")
- Single acting by banks when the crisis wahs in the wole project

Recommendations:

- Faster reaction to crisis situations based on often exercises and trainings
- Cooperation with peers in other banks in case of crisis situation

CYBER-EXE POLSKA 2013

Conclusions and recommendations for BANKING SECTOR

CONCLUSIONS

- Cooperation between banks in case of crisis situation is limited only to the basic information level

- There is a limited coordination of operational activities in both areas – technical and public relations. There was no common information issued to all e-banking customers even when the crisis was in the whole sector.

WNIOSKI

- 75% of responders (survey after the exercises) believe there is no a significant influence of common actions on the higher probability of crisis neutralization. Banks believe especially that there is no added value in cooperation in case of DDoS attacks

- There is very rare communication with the whole sector. If there is the information exchange it is only on the bank-to-bank level

WNIOSKI

- There is the information exchange platform for Polish banks, operated by Polish Banks Association. Not all banks used it during the crisis information.

- There was no communication between banks and Polish Financial Supervisory Authority during the crisis situation
  - The exercises gave the chance to clarify that the Authority does not expect this communication during the crisis situation but only after it.

WNIOSKI

- Not all banks have formal rules and procedures of communication with external parties
  - Other banks
  - Internet Service Providers
  - CERTs
  - LEAs
- There is big dependency of e-banking services availability on ISP services

RECOMMENDATIONS

- There is need for better cooperation between banks in case of sector wide crisis situation, especially banks need:
  - Rules for effective exchange of the operational information (logs, other relevant data)
  - Rules for operational help during crisis situation as well as areas of responsibilities
  - Establishing stable continuous cooperation between banks
  - Rules for reporting security incidents between banks as well as to the financial and state authorities.

CERT Role

- Very important in the banking incident response procedure
  - The banking sector mature regarding requesting for CERT services
  - Governmental CERT, commercial CERT services
- Operationaly involved in crisis management
  - DDoS support
  - Malware analysis
  - Other technical support
- The real check needs involvment of teams

It’s Hard Work but It’s Worth It!

CONTACT

Mirosław Maj
CEO

Cybersecurity Foundation
e-mail:
miroslaw.maj@cybsecurity.org

Maciej Pyznar
Senior Specialist

Government Centre for Security
e-mail:
maciej.pyznar@rcb.gov.pp

Cezary Piekarski
Senior Specialist

Deloitte Poland
E-mail:
cpiekarski@deloitteCE.com