Lessons learnt for CERT-s?
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 dedicated for the CIIP sector
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)
Organisational structure

Chief moderator

Evaluator

Technical Team

Media Team

Observers

Moderator - Bank 1

Moderator - Bank 2

Moderator - Bank 3

Moderator - Bank 4

Moderator - Bank 5

Moderator - Bank 6

Participant

Participant

Participant

Participant

Participant

Participant

PR Staff

PR Staff

PR Staff

PR Staff

PR Staff

PR Staff
The exercises objectives

- Checking the organisations’ cyber attack emergency response procedures
- Identification of interdependencies among banks, regulators and other entities within the financial sector
- Checking communication among banks, regulators and other entities within the financial market
Diagram 1.
Basic attack stages under DDoS path.

I PHASE of DDoS ATTACK
volumetric attack
application attack
media releases
communication between banks and
telecommunication operators, CERT teams and law enforcement agencies

II PHASE of DDoS ATTACK
volumetric attack
application attack
media releases

PHISHING ATTACK
collecting information from clients
cessation of the DDoS attack
use of customer data for criminal activities
customer complaints
escalation of media releases

BLACKMAILER’S ATTACK
communication with unit responsible for customer services
possible negotiations with blackmailer
APT ATTACK SCENARIO

ATTACK ANALYSIS
collecting as much information about the source of the attack as possible
escalation of media release
blackmail and possible negotiations

PUBLICATION OF CONFIDENTIAL INFORMATION
press release
residual confidential information
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 within banks
  - Organisational
  - Related to an external communication

- For implementing in the whole sector
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:
• Acquiring up-to-date knowledge
• 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

Conclusions:
- Prompt reaction to public news and customers’ “publications”
- Good coordination between internal PR team and crisis management unit
- Delayed reaction to “individual approach by journalists – („talking points”)”
- Single acting by banks when the crisis affects the whole project

Recommendations:
- Faster reaction to crisis situations based on often exercises and trainings
- Cooperation with peers in other banks in case of crisis situation
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.
• 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.
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
- Operationally involved in crisis management
  - DDoS support
  - Malware analysis
  - Other technical support
- The real check needs involvement 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