



Association  
des Banques  
et Banquiers  
Luxembourg



# Improving the security of e-banking systems a never ending story

INTERNET SECURITY DAY 2.0

8 May 2008

# Agenda



- Introduction
- Organisation
- Action plan
- Next steps
- Questions and Answers

# Agenda



- **Introduction**
- Organisation
- Action plan
- Next steps
- Questions and Answers

# Introduction (1)



- **Global Trends (1)**
  - Attacks on ICT systems and in particular on e-banking systems
    - not a new issue
    - not a fiction : reality outfaces fiction
    - not typical of the financial sector, but it is one of the most interesting targets for criminals
  - Attacking ICT Systems in general is an interesting market with an estimated annual “turnover” of some 2 billion € !

# Introduction (2)



- Global Trends (2)
  - Bad guys
    - we are moving away from the lonely hacker to black-hat hacker often member of criminal organisations
    - These criminal organisations succeed to “hire” highly qualified and ingenious ICT specialists

# Introduction (3)



- **Global Trends (3)**
  - Good Guys
    - a well organised and appropriated reaction is needed within a acceptable legal framework
    - Cooperation with various entities
      - potential targets of crime (e.g. bank customers, banks)
      - Law enforcement entities (e.g. police)
      - Supervisors
    - Internet is a technical and organisational matter requiring specific competences
    - Internet is a borderless “economical” space requiring international
    - Internet is characterized by the speed of moving data around : speedy reaction is of paramount importance

# Introduction (4)



- **What's happening in Luxembourg ? (1)**
  - Luxembourg is not an island : this applies to ICT Security as well :
    - Identity theft actions have been observed over the last last years :
    - Before 2007 : identity theft via more ore less sophisticated phishing
      - Emails requesting emails
      - Emails inviting customers to visit a (faked) bank site
    - Since 2007 :
      - Older techniques of phishing still quite common
      - Usage of “trojans” in conjunction with various techniques improving the “performance” of the attacks and reducing the risk to “be caught”.

# Introduction (5)



- What's happening in Luxembourg ? (2)
  - Tentatives or successes ?
    - Periodical attacks on different e-banking systems
      - e-banking sites
      - e-brokerage sites
    - Successful attacks on some accounts
    - Customers of several banks have been hit
    - Limited number and losses
  - ...nothing to worry about ?
    - Highly sensitive subject
    - Up to summer 2007, the Luxembourg banking community didn't handle these security issues in an efficient, coherent and coordinate way
    - Some banking associations throughout Europe organised over the last years to fight this type of crime

# Introduction (6)



- **ABBL ICT Security WG**

- A small group of ABBL member banks decided to react and to become proactive as well
- Why do banks have an interest to react ?
  - Time to act
    - still a limited number (?) of successful attacks
    - Still a limited financial impact
  - High risk of image and reputation loss
  - High risk of customers loosing confidence in the service
  - Great impact on organisation (front office/back office/ return to expensive “paper based” services)

# Introduction (7)



- **Re/acting is a complex task**
  - Sensitive information is handled
  - Detection processes of attacks are
    - complex to be implemented at the banks' level
    - difficult to be implemented at the customers' level (e.g. late detection of fraudulent transactions)
  - Competencies and resources for attack-analysis & attack-prevention :
    - unavailable and
    - inducing high costs
  - Numerous actors touched : customers (victims and mules); ISP; banks
  - Numerous actors want to have their say in the ICT security and e-banking security issues (banks, ABBL, CSSF, consumers' associations, Police, CASES, SRE, BCL, HCPN, etc.)

# Introduction (8)



- Pressure from banking supervisors and public authorities (1)
  - CSSF
    - « lettre circulaire dated 17 August 2007 » concerning « Information à la CSSF sur des fraudes et incidents en relation avec les services financiers par internet »
    - Rapport d'activité 2007
      - Asking for a review of currently used customer authentication mechanisms
      - Asking for a profiling process
  - ECB
    - 5th Progress Report on SEPA
    - « Need for continued work on security standards for payments »
    - « (...) The Eurosystem does not believe that it is appropriate to leave the scope of risk management entirely to the discretion of individual banks. (...) »

# Introduction (9)



- Pressure from banking supervisors and public authorities (2)
  - EC
    - Report on fraud regarding non cash means of payments in the EU (28 April 2008)
    - PSD : the Payment Services Directive to be implemented into national law and to come into force on 1st November 2009
      - New information requirements on payment instruments
      - New information requirements on the use of payment instruments
      - regulates the authorisation of payment instruments in order to reduce risks and consequences of unauthorised transactions
      - Regulates the processing of data for fraud prevention

# Agenda



- Introduction
- **Organisation**
- Action plan
- Next steps
- Questions and Answers

# Organisation (1)



- The organisation put into place takes into account the different stages of phishing attack (1)
  - Hiring of mules (money laundering : getting the money out of the initial transaction flow - e.g. use of Western Union)
  - Phishing e-banking access data
    - per exchange of emails
    - per fake websites,
    - by malware in a 2 step approach :
      - Uninsufficiently protected website will be modified (link to a criminal's site for a Trojan-downloader)
      - Uninsufficiently protected PC visiting infected website will permit the download.
      - Criminals are able to download any "useful" malware on that PC such as a keylogger

# Organisation (2)



- The organisation put into place takes into account the different stages of phishing attack (2)
  - On basis of collected or intercepted access data during stage 1, criminals initiate credit transfers
    - Single attacks
    - Sophisticated and orchestrated attacks using advanced technologies such as bot-nets
    - Man in the middle attacks
  - The mules execute money transfers with trace blurring...and become criminals too as they take part in a ML

# Organisation (3)



## Cooperation and Liaison

- Decision to cooperate with selected actors :
  - CSSF
  - Police
  - CASES
  - BCL (OCPG / HCPN)
  
- Decision to liaise with
  - Foreign banking associations (DE, FR, BE, UK)
  - Academic World (University of Luxembourg, CRP-HT, etc.)

# Organisation (4)



## Creation of 2 bodies (1)

- ICT Security working Group
  - Composed of representatives of some banks (BCEE, BR, DEXIA, EPT, FORTIS, ING, BdL, Paypal)
  - Membership guidelines inspired by the CPNI (Centre for the Protection of National Infrastructure in UK)
  - React and act (fight attacks and organise the reaction)
  - Act as FinAlert to be seen as a CERT / LERS (Computer Emergency Response Team / Local Emergency Response Structure) of the banking sector
  - Plan and coordinate the implementation of such structures which will interface the future Luxembourg “CERT structure” currently planned and set-up

# Organisation (5)



## Creation of 2 Working groups (2)

- E-banking Security Information exchange
  - Information Exchange Platform composed of representatives of banks offering e-banking services and likely to be hit by attacks
  - Interested banks met for the first time in August 2007
  - Quarterly meetings
  - Meetings on Urgencies
  - Lack of interest / resources
  - Merging the 2 bodies to reduce redundancy of information and work

# Agenda



- Introduction
- Organisation
- **Action plan**
- Next steps
- Questions and Answers

# Action Plan (1)



The ICT Security Working Groups adopted an action plan based on 4 axes

1. Emergency reactions and actions
2. Information and Education
3. Liaisons
4. Research

# Action Plan (2)



## 1. Emergency reactions and actions (1)

- Organisation of emergency meetings
- Definition of measures to be taken
  - Bank level
  - Banking community level / escalation > CERT/HCPN
  - Lessons learned / security solutions to be implemented immediately
- Limited FinAlert (CERT/LEERS) role
  - Definition of an emergency procedure (together with CASES/CERT, police and CSSF) comprising recommended customer's behaviour
- Planning and implementation of the FIN-CERT/LEERS
  - Project (services)
  - Implementation "framework" (structure, operations)

# Action Plan (3)



## 1. Emergency reactions and actions (2)

- Elaborating best practice security measures at the banks' level
  - Making the system non attractive
    - Application based limits
  - Monitoring 24/24 - global supervision of the Internet
    - Monitoring of the net
      - Scanning of newsgroups, mail-lists, web-logs
      - News services
      - Discussion forums
    - Searching information on phishing techniques and banks
    - Automatic checking of suspicious URL
    - Collecting SPAMs
      - Spam honey pots

# Action Plan (4)



## 1. Emergency reactions and actions (3)

- Analysis of detected malware
  - Studying functioning, proliferation, potential of risk
  - Tracking back of attacks
  - Cooperation with anti-virus development communities
- Anti-phishing tools
- Documentation of incidents for forensic purposes
- Communicating within the banking community and exchanging relevant information (e.g. IP addresses, suspicious beneficiaries' account)
- Fighting of suspicious Domains and hosting
  - Servers containing fake Web-pages
  - Servers where malware send "phished" data
  - Registration
  - Poisoning (counterattacking)
- Cooperation - outsourcing to highly specialised service companies

# Action Plan (5)



## 2. Information and Education

- Customers
  - Press releases (in cooperation with CASES)
  - Leaflets and documentations (in cooperation with CASES)
  - Information campaign (in cooperation with CASES and Police)
  - Presence at public events (in cooperation with CASES)
- Banks
  - Sponsoring of hack.lu / phishing workshop
  - IFBL - training sessions for e-banking help desk staff, tellers, back-office people in contact with e-banking customers
  - IFBL - training sessions for ICT security and security experts
- Seminars and conferences

# Action Plan (6)



## 3. Liaisons

- Banking Communities or associations abroad
  - DE - BdB
  - DE - BVR
  - DE - DSGV
  - FR - FBF
  - EBF
- Others
  - BCL (OCPG / HCPN)

# Action Plan (7)



## 4. Research

- Université de Luxembourg
- CRP HT
- Other Universities

# Agenda



- Introduction
- Organisation
- Action plan
- **Next steps**
- Questions and Answers

# Next Steps (1)



- ICT Security Working Group
  - Review of recommendations for banks (taking into account CSSF's observations)
  - Emergency procedure (CASES and Police implication)
  - Clarification of data protection issues
  - Mutualised monitoring and active services : the FinAlert Project
- Information
  - Information Campaign (under study)
  - Hack.lu 2008
  - Various Messages
  - Information Campaign using newspaper media

# Agenda



- Introduction
- Organisation
- Action plan
- Next steps
- Questions and Answers

# Questions and Answers



?

?

?

?

?

?

?

# ... the End



Is this the end really ? No !

You should be convinced by now that banks are living a never ending story :

Atréjus and Furchurs are welcome to fight the evil !

Thank you for your interest and attention

Marc HEMMERLING  
Hemmerling@abbl.lu