That's weird! Many security measures have few effect in Japan

～ Light & Shadow ～

@ AVTOKYO2013.5

AIDO & Manaka

Translation : Kazuki Yonezawa

Agenda

- Background
- Encrypting email attachments
- " Trial" for Internal fraud detection by integrated log management
- Personal belongings check at Data Center
- Intelligent Office Buildings
- Entry & Exit management by ID cards
- Summary & Conclusion

Background

- Security measures tend to come with cost and “ sacrifice” of convenience,
- But sometimes such cost and “ sacrifice” become unreturned,
- This session will introduce such unreturned measures.

Encrypting email attachments

Light Effects can be expected

- “ hot” , since PIP Act enforcement.
- Email is “ post card” ; risk of information breach on the way
- Encryption should be solution
- Encrypt automatically on the server, then send password by separate email; encryption without any exception
- Even exe file can be sent by changing to “ ex_” or “ ex e” to “ overcome” mail attachment filtering

Encrypting email attachments

Shadow *Unreturned and Side effect*

- Sending password from same server and on the same route does not prevent eavesdropping
- Eavesdropping on the route can be done ONLY by NSA?
- Automatic encryption encrypts malware also; help them to reach endpoints directly
- Easiest way to have users run .exe file
- " Surest vehicle" for spear phishing attack

“ Trial” for Internal fraud detection by integrated log management

Light Effects can be expected

- Tough challenge for Internal Control
- Privileged accounts can do everything.
- Manipulating financial statement by the accounts should be serious problem
- Operation with the accounts must be under surveillance
- Caution by collecting and “ preserving” all operating logs
- Record mouse operation by movie

" Trial" for Internal fraud detection by integrated log management

Shadow Unreturned and Side effect

- Serious manipulation of financial statement is done by managements
- Operators have never been involved such problem
- Operators don' t know what to do, data content, in spite of privileges
- Managements to decide budget, or consultants to propose scheme, tend to do/miss such manipulation
- Surveillance for wrong target
- Just resulted in increased work

Personal belongings check at Data Center

Light *Effects can be expected*

- Information disclosure guidelines in accordance with the safety and reliability of the data center (Ministry of Internal Affairs and Communications)
- Prohibit to bring in recordable media, USB memory, and mobile phone
- Mobile phone with camera is strictly prohibited (even resulted in developing feature phones without camera for business use)
- Application form, snap inspection, lockers, limited to use only clear plastic bag, and so on
- Even uniform without any pockets, for operators

Personal belongings check at Data Center

Shadow *Unreturned and Side effect*

- Can bring in by hiding in clothes or underwear or socks, IN ANY WAY; “ they make effort”
- Enforcement only to whom comply the rule
- Effective to caution, but not to overconfident nor apply excessively
- Should result in increased work for innocents with missing malicious acts

Intelligent Office Buildings

Light *Effects can be expected*

- " physical access control" , requirement of ISO27000 and/or PCIDSS
- Security gates, entry controlled doors, and elevators with ID cards authentication to control access to floors
- Emergency stairs have also entry control and covers couriers too
- Large nice cafeteria (like google) to help staying in the office area for not to have lunch and drink alcohol outside.
  (avoid problems caused by drinking.
  ex. Lost briefcase with documents, ID Card)

Intelligent Office Buildings

Shadow *Unreturned and Side effect*

- Glass-walled buildings allow to see displays and whiteboards from the buildings around
- Tend to be smoke-free; no " social interaction space" for smokers
- Smokers go outside
- Making phone call at smoking space is not unusual
- Phone conversation at smoking place could be information leakage

Here is Marunouchi
(Location of many headquarters of famous companies in Japan)

Social interaction smoking space for executives outside

Entry & Exit management by ID cards

Light Effects can be expected

- " Physical and Environmental Security Management" of ISO27000
- Control physical entry by security gates and/or entry controlled doors
- Prevent piggy back at security gates to protect data center

Entry & Exit management by ID cards

Shadow *Unreturned and Side effect*

- Large buildings tend to be multi-tenanted, thus hard to equip security gates but entry controlled doors
- Entry controlled doors allow piggy back
- changed to the fingerprint authentication from the IC card authentication, allow piggy back as well
- Easy to do especially, around begin/end of lunch time and regulated quitting time
- Restrooms are not entry controlled at most of the cases
- Can wait for someone at restroom by brushing teeth

Risk of ID cars selves

+Shadow Unreturned and Side effect

- Go out for lunch at Otemachi area (Location of many headquarters of famous large Bank)
- ID card straps shows corporate logos, peoples are taking lunch with them
  They had serious information related to the management
- Conversation could cause serious information breach
- Press is " camping" to take such information especially upon incidents M&A, or even rumor
- No companies request employees to take off straps outside of office
- If requested, some of them should lose ID cards
- Going out with showing one' s name and company should be targeted by social engineering attackers

Summary & Conclusion

Unreturned security measures

- Blind belief to encrypting everything to prevent information breach includes eavesdropping
- Blind belief to IC cards/fingerprints, because they are unable to forge (do not consider daily usage)
- Mansplaining surveillance and prohibiting to field operations by managements with arrogant attitude
- Blind acceptance of cutting edge/expensive technologies/technique (consider only with cost not performance)
- Security measures of " do what others do"

As the result, expensive measures become unreturned!

Do not implement any measures without performance.

Do only measures which brings appropriate return!!

Thank you for listening

e-mail : aido@hkg.odn.ne.jp
Facebook : Hiroshi.Aido 相戸 浩志