PROTECTION ET PÉRENNISATION DU PATRIMOINE SCIENTIFIQUE NUMÉRIQUE D'UN LABORATOIRE DE RECHERCHE

CYRIL BRAS

CESAR2017@CYRIL-BRAS.FR

RENNES, 27/11/2017

PLAN

- Context
- Data flow management and protection
- Data perpetuation
- IT security training and information
- Prospect
- Conclusion

PLAN

- Context
- Data flow management and protection
- Data perpetuation
- IT security training and information
- Prospect
- Conclusion

CONTEXT

- CERMAV :
  - CNRS unit
  - Located in Grenoble Campus Universitaire
  - Workforce : ~120 persons
  - IT Service :
    - 3 persons
    - 6 IT correspondents
  - ~200 computers (scientific data generator included)
  - ~30 servers, some of them in DMZ (Web sites, emails, DNS…)

CONTEXT

- Particularities :
  - Each laboratory IT is independent and is placed under the unit director responsability
  - Researchers interact and exchange data with outsiders

CONTEXT

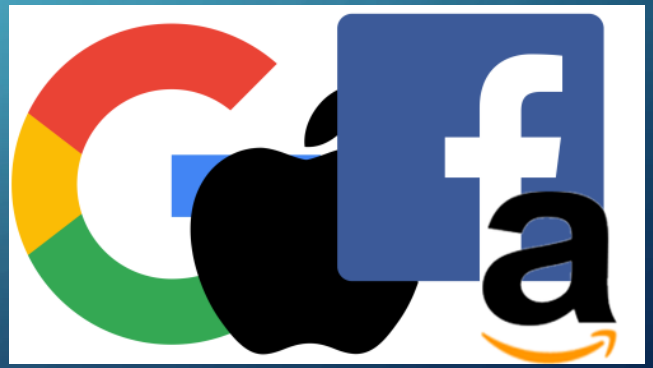
- Objective :
  - Protect data from accidental or malicious damage
- How :
  - Data flow management and protection
  - Data perpetuation
  - Staff training and informing about healthy IT usage and how to structurate data

PLAN

- Context
- Data flow management and protection
- Data perpetuation
- IT security training and information
- Prospect
- Conclusion

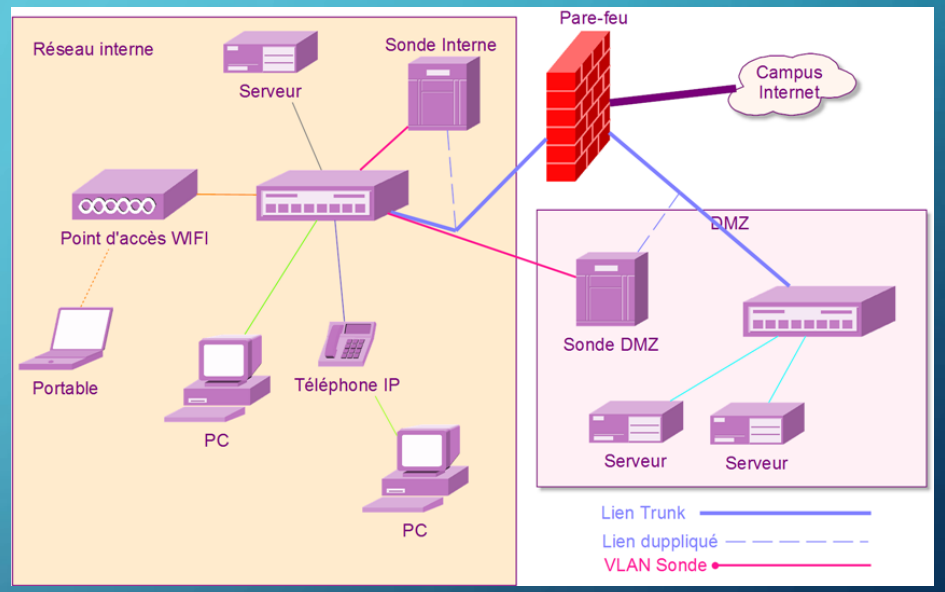
DATA FLOW MANAGEMENT AND PROTECTION

- Ascertainment
  - Flow filtering rules only based on IP adresses, port number and/or protocol are **outdated**
  - Public cloud offers **opulence** is a daily reality
  - Proposing services as attractives and efficient as GAFA services is really hard for IT teams



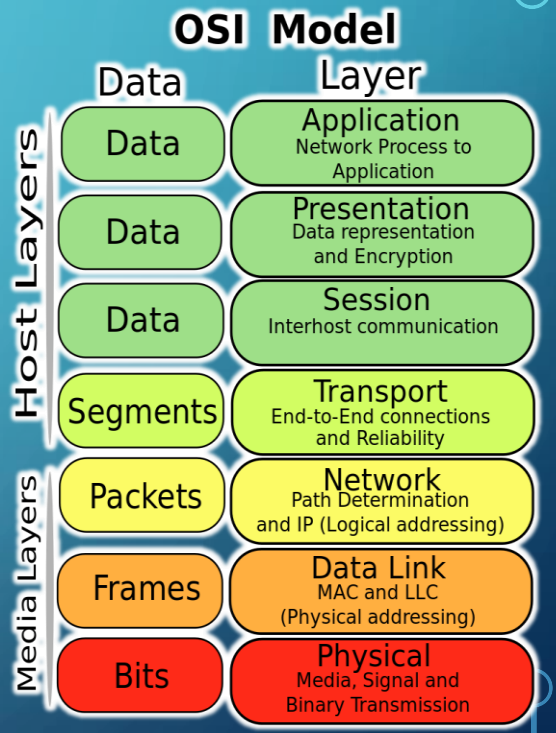
DATA FLOW MANAGEMENT AND PROTECTION

- What to do ?
  - First step : deploying Intrusion Detection System (IDS)
    - Detection of public cloud solution usage
  - Deploying our private cloud service (Owncloud)
    - Staff still using public cloud services
  - Trying to avoid access to public cloud services
    - Difficulty : a lot of different changing IP adresses to deny



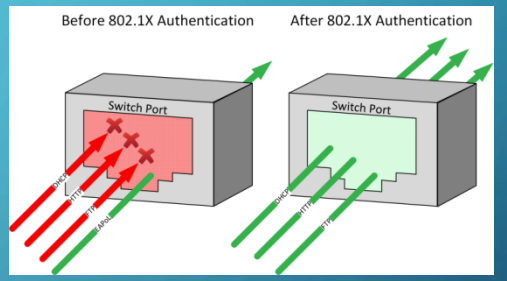
DATA FLOW MANAGEMENT AND PROTECTION

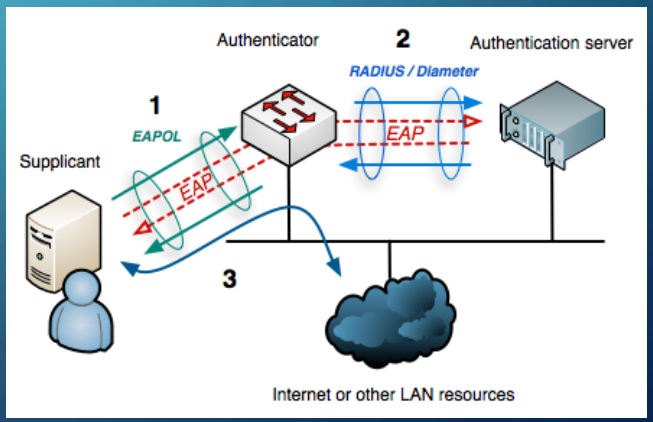
- What to do ?
  - Next Generation firewall deployment (Palo-Alto)
    - Firewall rules applied on application layer
      - Ex : Facebook publishing denied but browsing allowed
      - Ex : Use of outbound mail server is forbidden (gmail…)
      - Ex : Allowing access for a specific user not only a computer or an IP address



DATA FLOW MANAGEMENT AND PROTECTION

- What to do ?
  - Legitimate network access guaranted by 802.1x security standard
    - Sensitive data access is only possible from an authorized device
    - Control access to the network
    - VLAN to separate activities





DATA FLOW MANAGEMENT AND PROTECTION

- What to do ?
  - Beware of multifunctions copiers
    - Limit document scan to internal e-mail server
    - Isolate them from the rest of the network

PLAN

- Context
- Data flow management and protection
- Data perpetuation
- IT security training and information
- Prospect
- Conclusion

DATA PERPETUATION

- Why ?
  - In case of cyber attacks data can be damaged or destroyed
  - Data loss could have an impact on scientific activities (acquisition data, publications in writing…)

DATA PERPETUATION

- How, for IT team ?
  1. Acquire the necessary equipment to save our data without human intervention (LTO-6 library with 9 places for cartridges)
  2. Configure the software to control backup devices (Open source : Bacula)
  3. Define a backup plan (3 months for current data retention and 1 year for archiving)
  4. Plan data restore test

DATA PERPETUATION

- How, for users ?
  1. Make difference between personnal and scientific or technical data
  2. Automatic folder synchronization from local computer to server area
  3. Structure the data according to an internal procedure (raw or processed data, scientific communication…)

PLAN

- Context
- Data flow management and protection
- Data perpetuation
- IT security training and information
- Prospect
- Conclusion

IT SECURITY TRAINING AND INFORMATION

- Every user is a part of the IT security chain
- Almost of nowadays security issues concern final users
- How to ?

IT SECURITY TRAINING AND INFORMATION

- CERMAV IT security information
  - Every new staff member is educated to IT security good practise (~10 sessions per year)
  - All CERMAV employees are educated and informed about IT security (~2 times a year)
    - DGSI : scientific data protection
    - RSSI from CNRS, Université Grenoble Alpes
    - CSSI

IT SECURITY TRAINING AND INFORMATION

- CERMAV IT security information
  - National IT security alerts are « translated » to users, what to do… (apply updates…)
  - When necessary, we remind users how to act (ex : in case of a virus infection…)

IT SECURITY TRAINING AND INFORMATION

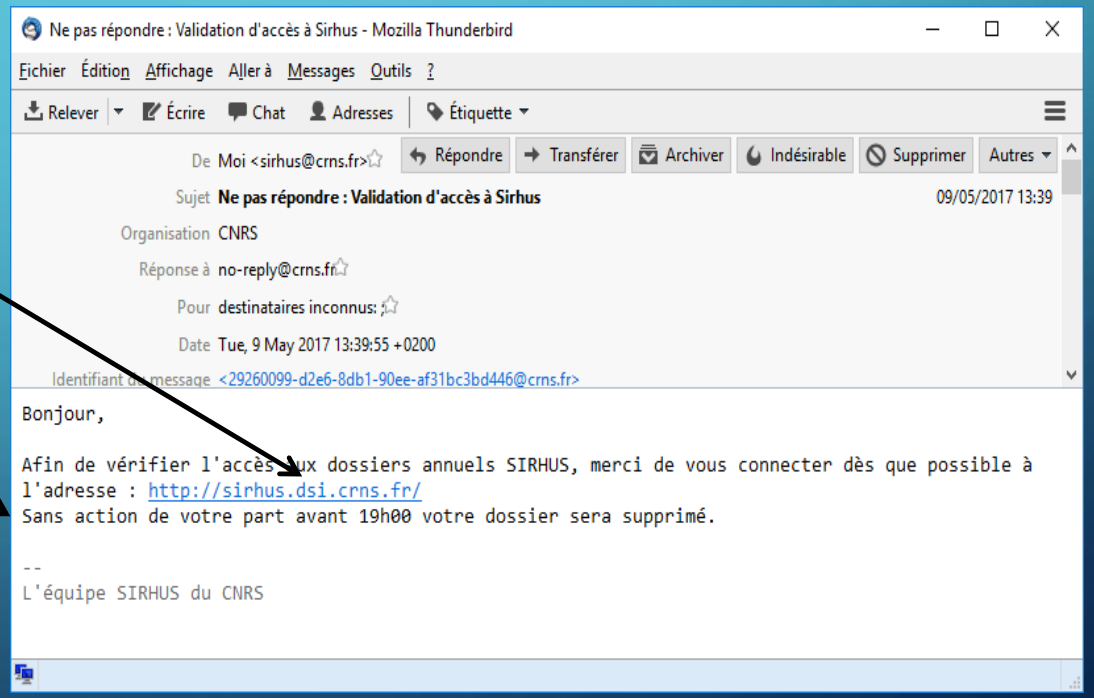
- CERMAV IT security training, example of spearphishing exercise
  1. Context : every year, CNRS is launching a national campaign for technical and administrative staff promotion.
     - Few years ago crns.fr domain name was declared and we received an alert about it
     - Declaration of this domain name on our internal DNS server
     - Making a clone of the CNRS official promotion campaign website to be used for the spearphishing attack
     - Using of Social Engineering Toolkit to drive the attack and to test browser vulnerabilities

IT SECURITY TRAINING AND INFORMATION

2. Sending an e-mail with the usual aspect of e-mails sent as part of CNRS promotion campaign and containing a link to an address in crns.fr.

False address pointing to attacker server

Social pressure



IT SECURITY TRAINING AND INFORMATION

- What do we observe ?
  - Few seconds after e-mail was sent, 7 users clicked on the link
  - At the same time, 5 users reports suspected e-mail and requested for an alert to be sent
  - All the 7 webbrowsers used were up to date and have no vulnerabilities

IT SECURITY TRAINING AND INFORMATION

- What have we done after ?
  - Exercise review at a general staff meeting
  - A good opportunity to concretely support the need to be vigilant when receiving emails even when they seem legitimate.
  - Positive feedback from users

PLAN

- Context
- Data flow management and protection
- Data perpetuation
- IT security training and information
- Prospect
- Conclusion

PROSPECT

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

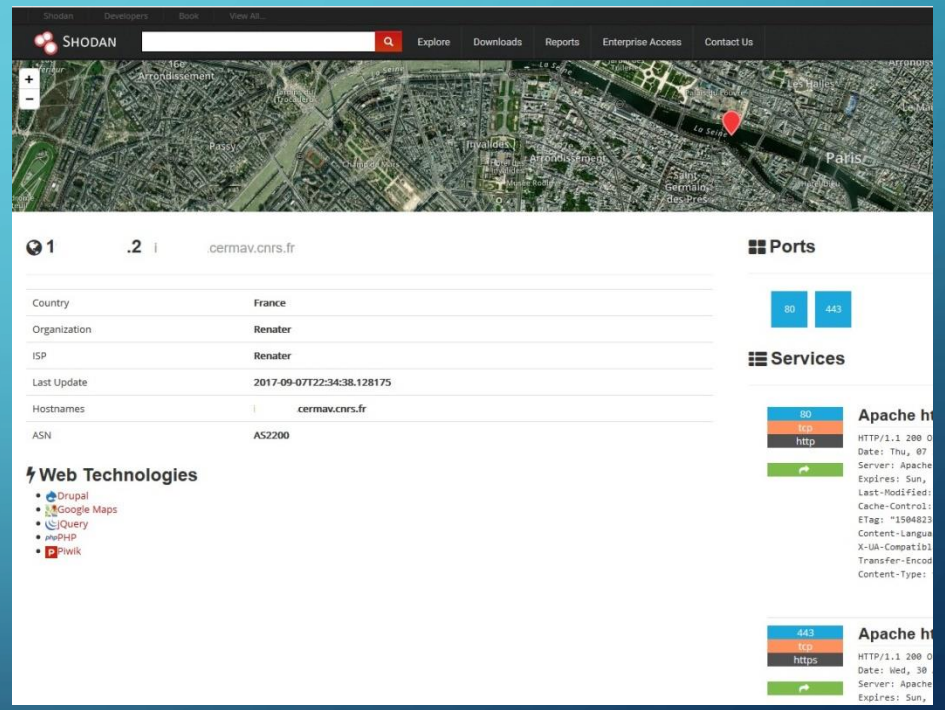
Sun Tzu, The Art of War

PROSPECT

- Except internals cyber exercises, CERMAV was never involved in any larger exercise :
  - GIP Renater (Internet provider for french scientific research) is providing to CISO some tools to look for vulnerabilities
  - Important to know weak point

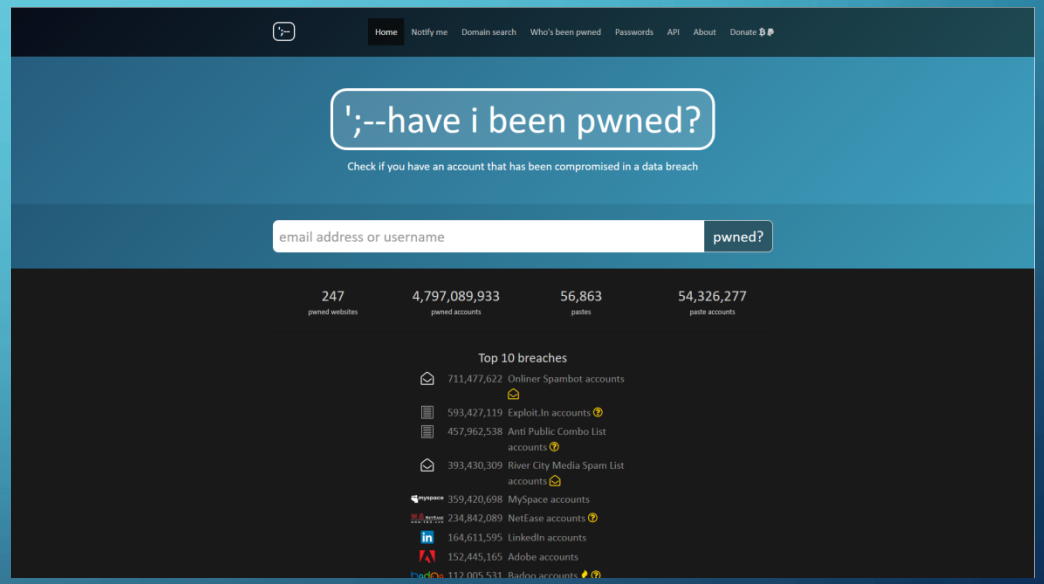
PROSPECT

- A way to drive some tests from outside :
  - Shodan search engine applied on our public IP address ranges



PROSPECT

- A way to drive some tests from outside :
  - Check compromised account databases to see if CERMAV users accounts are in.



PROSPECT

- Fine-tuning anomaly detection could be based on the use of a SIEM (Security Information and Event Management).
- From users point of view, exercices and information combined to the news about IT security incidents (ex : Wannacry, Petia…) have a benefic effect on the collective awareness about IT security importance.

PLAN

- Context
- Data flow management and protection
- Data perpetuation
- IT security training and information
- Prospect
- Conclusion

CONCLUSION

- Data flows
  - Are not limited to technical solutions
  - Require involvment of all IT actors
- Data organization can’t be done efficiently without relying on human factor

CONCLUSION

- Human factor had to be integrated in all security solutions
  - To become an essential link of protection
  - To maintain confidence in the use of digital technologies

QUESTIONS ?


C&ESAR 2017
LA PROTECTION DES DONNÉES
FACE À LA MENACE CYBER


cnrs


Cermav