



# La sécurisation des données (accès, sauvegarde, archivage...)



Cyril Bras [cyril.bras@cermav.cnrs.fr](mailto:cyril.bras@cermav.cnrs.fr)  
Grenoble 16/10/2017



# Introduction

- › Définitions de la donnée
- › Cybersécurité, qu'est ce que c'est ?
- › Les menaces qui peuvent affecter les données
- › Quelques solutions et outils
- › Conclusion



# Introduction

- › Définitions de la donnée
- › Cybersécurité, qu'est ce que c'est ?
- › Les menaces qui peuvent affecter les données
- › Quelques solutions et outils
- › Conclusion



# La donnée

## » Définition générale :

– Une donnée est un ensemble de valeurs faisant référence à la représentation et au codage d'une information ou un savoir sous une forme adaptée à un usage. Une donnée n'est pas une information. Une donnée requiert une interprétation pour devenir une information.

```

atmel_at76c502_3com.bin      ctfw-3.0.0.0.bin      iwlwifi-5000-5.ucode    ql2100_fw.bin
atmel_at76c502_3com-wpa.bin ctfw-3.0.3.1.bin      iwlwifi-5150-2.ucode    ql2200_fw.bin
atmel_at76c502_3com-wpa-wpa.bin ctfw-3.1.0.0.bin      iwlwifi-6000-4.ucode    ql2300_fw.bin
atmel_at76c502d-wpa.bin      ctfw-3.2.1.0.bin      iwlwifi-6000g2a-5.ucode ql2322_fw.bin
atmel_at76c502d-wpa-wpa.bin  ctfw-3.2.1.1.bin      iwlwifi-6000g2a-6.ucode ql2400_fw.bin
atmel_at76c502e.bin          ctfw-3.2.3.0.bin      iwlwifi-6000g2b-6.ucode ql2500_fw.bin
atmel_at76c502e-wpa.bin      ctfw.bin               iwlwifi-6050-4.ucode    qllogic
atmel_at76c502-wpa.bin       cxgb3                   iwlwifi-6050-5.ucode    r128
atmel_at76c503-i3861.bin     cxgb4                   iwlwifi-7260-10.ucode   radeon
atmel_at76c503-i3863.bin     dabusb                  iwlwifi-7260-12.ucode   README.atmel-firmware
atmel_at76c503-i3863-fwd3c.bin ds56k                    iwlwifi-7260-13.ucode   README-usb.atmel-firmware
atmel_at76c503-i3863-fwd3c-wpa.bin ds56k-wpa                iwlwifi-7260-16.ucode   rt2561.bin
atmel_at76c504_2958-wpa.bin  edgeport                 iwlwifi-7260-7.ucode    rt2561s.bin
atmel_at76c504a_2958-wpa.bin em26                      iwlwifi-7260-9.ucode    rt2561b.bin
atmel_at76c504c-wpa.bin     ess                      iwlwifi-7265-11.ucode   rt2870.bin
atmel_at76c504c-wpa-wpa.bin  ess-wpa                  iwlwifi-7265-12.ucode   rt2870b.bin
atmel_at76c505-fwd2958.bin   htc_9271.fw             iwlwifi-7265-15.ucode   rt2870c.bin
atmel_at76c505-fwd2958-wpa.bin htc_9271-wpa            iwlwifi-7265-16.ucode   rt2870d.bin
atmel_at76c505-fwd2958-wpa-wpa.bin htc_9271-wpa-wpa        iwlwifi-7265-9.ucode    rt2870e.bin
atmel_at76c505-wpa.bin      ipw2100-1.3.fw          iwlwifi-7265D-12.ucode  sb16
atmel_at76c505-wpa-wpa.bin  ipw2100-1.3-wpa.fw     iwlwifi-7265D-13.ucode  sb16-wpa
av7110                       ipw2100-1.3-p.fw       iwlwifi-7265D-16.ucode  teluti
b43-open                     ipw2100-1.3-wpa-wpa.fw iwlwifi-8000C-13.ucode  ti_3410.fw
bnx2                           ipw2200-1.fw           iwlwifi-8000C-16.ucode  ti_5052.fw
bnx2x                         ipw2200-sniffer.fw     kaweth                   tigon
bnx2x-el-5.2.13.0.fw         isci                    keyspan                  tr_smctr.bin
bnx2x-elh-5.2.13.0.fw       ivtv-firmware-license-end-user.txt keyspan_pda              ttusb-budget
brcm                           ivtv-firmware-license-oemihvisv.txt korg                     usb8388.bin
carl9170-1.fw                iwlwifi-1000-3.ucode   LICENSE.ipw2100         v41-cx2341x-dec.fw
cbfw-3.0.0.0.bin              iwlwifi-1000-5.ucode   LICENSE.ipw2200-fw     v41-cx2341x-enc.fw
cbfw-3.0.3.1.bin              iwlwifi-100-5.ucode    LICENSE.usb8388        v41-cx2341x-init.mpg
cbfw-3.1.0.0.bin              iwlwifi-105-6.ucode    matrox                  v41-cx25840.fw
cbfw-3.2.1.0.bin              iwlwifi-135-6.ucode    microcode.dat           v41-pvrusb2-24xxx-01.fw
cbfw-3.2.1.1.bin              iwlwifi-2000-6.ucode   mts_cdma.fw            v41-pvrusb2-29xxx-01.fw
cbfw-3.2.3.0.bin              iwlwifi-2030-6.ucode   mts_edge.fw            vicam
cbfw.bin                      iwlwifi-3160-10.ucode  mts_gsm.fw             whiteheat.fw
cis                            iwlwifi-3160-12.ucode  mts_mt9234mu.fw        whiteheat_loader.fw
COPYING.atmel-firmware        iwlwifi-3160-13.ucode  mts_mt9234zba.fw       yam
COPYRIGHT-usb.atmel-firmware iwlwifi-3160-16.ucode  myril0ge_ethp_z8e.dat   yamaha
cpia2                         iwlwifi-3160-7.ucode   myril0ge_eth_z8e.dat    zd1211

```





# La donnée

## De recherche ou scientifique :

— des enregistrements factuels (chiffres, textes, images et sons), qui sont utilisés comme sources principales pour la recherche scientifique et sont généralement reconnus par la communauté scientifique comme nécessaires pour valider des résultats de recherche »

atmel_at76c502_3com.bin	ctfw-3.0.0.0.bin	iwlwifi-5000-5.ucode	ql2100_fw.bin
atmel_at76c502_3com-wpa.bin	ctfw-3.0.3.1.bin	iwlwifi-5150-2.ucode	ql2200_fw.bin
atmel_at76c502d-wpa.bin	ctfw-3.1.0.0.bin	iwlwifi-6000-4.ucode	ql2300_fw.bin
atmel_at76c502d-wpa.bin	ctfw-3.2.1.0.bin	iwlwifi-6000g2a-5.ucode	ql2322_fw.bin
atmel_at76c502d-wpa.bin	ctfw-3.2.1.1.bin	iwlwifi-6000g2a-6.ucode	ql2400_fw.bin
atmel_at76c502e.bin	ctfw-3.2.3.0.bin	iwlwifi-6000g2b-6.ucode	ql2500_fw.bin
atmel_at76c502e-wpa.bin	ctfw.bin	iwlwifi-6050-4.ucode	glogic
atmel_at76c502-wpa.bin	csrb3	iwlwifi-6050-5.ucode	r128
atmel_at76c503-i3863.bin	csig	iwlwifi-7260-10.ucode	radeon
atmel_at76c503-i3863.bin	dabusb	iwlwifi-7260-12.ucode	README.atmel-firmware
atmel_at76c503-rfmd-acc.bin	drp56k	iwlwifi-7260-13.ucode	README-usb.atmel-firmware
atmel_at76c504-2958-wpa.bin	edgeport	iwlwifi-7260-16.ucode	rt2561s.bin
atmel_at76c504-wpa.bin	ess	iwlwifi-7260-7.ucode	rt2561s.bin
atmel_at76c504-wpa.bin	ess	iwlwifi-7265-10.ucode	rt2860.bin
atmel_at76c504-wpa.bin	ess	iwlwifi-7265-12.ucode	rt2870.bin
atmel_at76c505-gsm-fw	htc_9271.fw	iwlwifi-7265-13.ucode	rt3200.bin
atmel_at76c505-rfmd2958.bin	htc_9271.fw	iwlwifi-7265-16.ucode	rt73.bin
atmel_at76c505-wpa.bin	intelliport2.bin	iwlwifi-7265-17.ucode	rtw2870
atmel_at76c506.bin	ipw9100-1.3.fw	iwlwifi-7265D-10.ucode	rtw2870
atmel_at76c506-wpa.bin	ipw2100-1.3-i.fw	iwlwifi-7265D-12.ucode	sbl6
atmsarl1.fw	ipw2100-1.3-p.fw	iwlwifi-7265D-13.ucode	sun
av7110	ipw2200-bss.fw	iwlwifi-7265D-16.ucode	tehuti
b43-open	ipw2200-ibss.fw	iwlwifi-8000C-13.ucode	ti_3410.fw
bnx2	ipw2200-sniffer.fw	iwlwifi-8000C-16.ucode	ti_5052.fw
bnx2x	iscsi	kaweth	tigon
bnx2x-el-5.2.13.0.fw	ivtv-firmware-license-end-user.txt	keyspan	tr_smctr.bin
bnx2x-elh-5.2.13.0.fw	ivtv-firmware-license-oemihvisv.txt	keyspan_pda	ttusb-budget
brcm	iwlwifi-1000-3.ucode	korg	usb8388.bin
carl9170-1.fw	iwlwifi-1000-5.ucode	LICENSE.ipw2100	v41-cx2341x-dec.fw
cbfw-3.0.0.0.bin	iwlwifi-100-5.ucode	LICENSE.ipw2200-fw	v41-cx2341x-enc.fw
cbfw-3.0.3.1.bin	iwlwifi-105-6.ucode	LICENSE.usb8388	v41-cx2341x-init.mpg
cbfw-3.1.0.0.bin	iwlwifi-135-6.ucode	matrox	v41-cx25840.fw
cbfw-3.2.1.0.bin	iwlwifi-2000-6.ucode	microcode.dat	v41-pvrusb2-24xxx-01.fw
cbfw-3.2.1.1.bin	iwlwifi-2030-6.ucode	mts_cdma.fw	v41-pvrusb2-29xxx-01.fw
cbfw-3.2.3.0.bin	iwlwifi-3160-10.ucode	mts_edge.fw	vicam
cbfw.bin	iwlwifi-3160-12.ucode	mts_gsm.fw	whiteheat.fw
cis	iwlwifi-3160-13.ucode	mts_mt9234mu.fw	whiteheat_loader.fw
COPYING.atmel-firmware	iwlwifi-3160-16.ucode	mts_mt9234zba.fw	yam
COPYRIGHT-usb.atmel-firmware	myril0ge_ethp_z8e.dat	myril0ge_ethp_z8e.dat	yamaha
cpia2	myril0ge_eth_z8e.dat	myril0ge_eth_z8e.dat	zdl211





# Introduction

- › Définitions de la donnée
- › Cybersécurité, qu'est ce que c'est ?
- › Les menaces qui peuvent affecter les données
- › Quelques solutions et outils
- › Conclusion

# Cybersécurité

## › Définition :

- On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour **protéger le cyberenvironnement et les actifs des organisations et des utilisateurs**. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement.



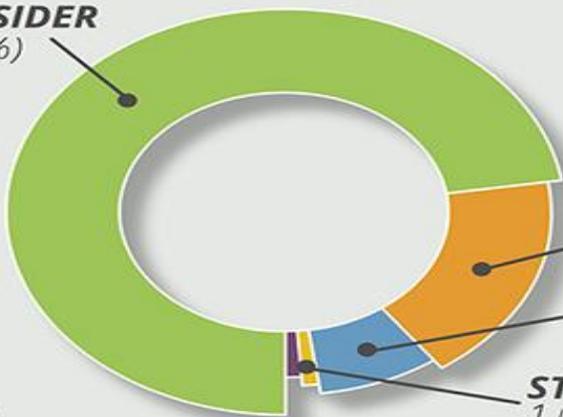
# Cybersécurité

- › Quelques chiffres pour 2017 à l'échelle mondiale (source : Helpnetsecurity Number of lost, stolen or compromised records increased by 164%)
  - Augmentation de 164% des pertes, vol ou compromission de données par rapport à 2016
  - Augmentation de 4000% dans l'environnement éducation

## NUMBER OF BREACH INCIDENTS BY SOURCE

### FIRST HALF OF 2017

**MALICIOUS OUTSIDER**  
679 INCIDENTS (74%)



**ACCIDENTAL LOSS**  
166 INCIDENTS (18%)

**MALICIOUS INSIDER**  
71 INCIDENTS (8%)

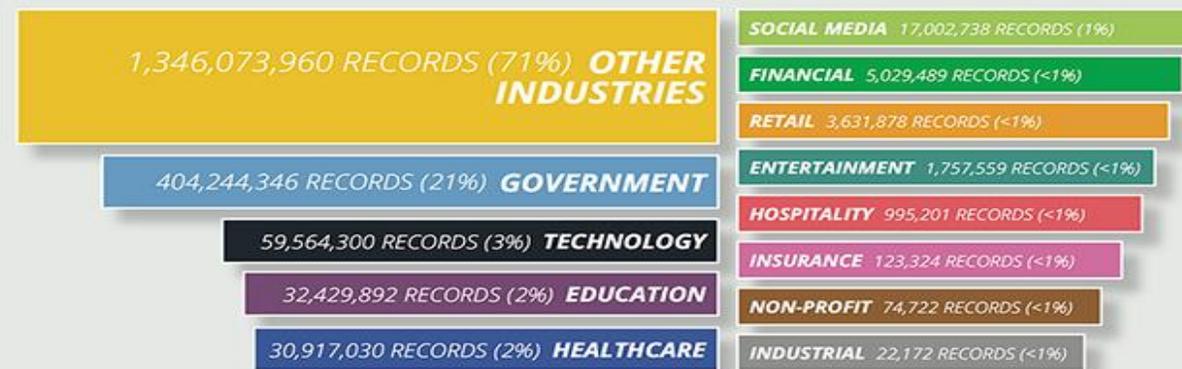
**STATE SPONSORED**  
1 INCIDENT (<1%)

**918**  
TOTAL BREACHES  
1 UNKNOWN INCIDENT

Source: BREACHLEVELINDEX.COM  
January 2017 to June 2017

## NUMBER OF RECORDS BREACHED BY INDUSTRY

### IN FIRST HALF OF 2017



**1,901,866,611** TOTAL RECORDS

Source: BREACHLEVELINDEX.COM  
January 2017 to June 2017



# Cybersécurité

- › Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- › 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C.

Bien à protéger



## Disponibilité

Propriété d'**accessibilité au moment voulu** des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues)

## Intégrité

Propriété d'**exactitude et de complétude** des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

## Confidentialité

Propriété des biens de **n'être accessibles qu'aux personnes autorisées**

# Cybersécurité

- › Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- › 1 critère complémentaire est souvent associé au D.I.C.

Bien à protéger



## Preuve

Propriété d'un bien permettant de retrouver, avec une **confiance suffisante**, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe  
Notamment :

La **traçabilité** des actions menées

L'**authentification** des utilisateurs

L'**imputabilité** du responsable de l'action effectuée

# Cybersécurité

« Sûreté » et « Sécurité » ont des significations différentes en fonction du contexte. L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun.

## Sûreté

Protection contre les dysfonctionnements et accidents involontaires

Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.

Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)

Parades : sauvegarde, dimensionnement, redondance des équipements...

## Sécurité

Protection contre les actions malveillantes volontaires

Exemple de risque : blocage d'un service, modification d'informations, vol d'information

Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts

Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage...

# Cybersécurité

Ainsi, pour évaluer si un bien est correctement sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Preuve. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.

L'expression du besoin attendu peut-être d'origine :

- › **Interne** : inhérente au métier de l'entreprise
- › ou **externe** : issue des contraintes légales qui pèsent sur les biens de l'entreprise.

Exemple des résultats d'un audit sur un bien sur une échelle (Faible, Moyen, Fort, Très fort) :



Niveau de Disponibilité du bien	Très fort
Niveau d'Intégrité du bien	Moyen
Niveau de Confidentialité du bien	Très fort
Niveau de Preuve du bien	Faible



Le bien bénéficie d'un niveau de sécurité adéquat

LA SÉCURISATION DES DONNÉES (ACCÈS, SAUVEGARDE, ARCHIVAGE...)

# Cybersécurité

- › Tous les biens d'un S.I. n'ont pas nécessairement besoin d'atteindre les mêmes niveaux de DICP.
- › Exemple avec un site institutionnel simple (statique) d'une entreprise qui souhaite promouvoir ses services sur internet :

**Disponibilité = Très fort**

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaître ses services au public

**Intégrité = Très fort**

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable)



Serveur  
web

**Confidentialité = Faible**

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

**Preuve = Faible**

Un faible niveau de preuve suffit. En effet, ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

# Cybersécurité

Un Système d'Information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer de garantir les propriétés DICP sur les biens de ce S.I. Voici quelques exemples de mécanismes de sécurité participant à cette garantie :

		D	I	C	P
<b>Anti-virus</b>	Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité	✓	✓	✓	
<b>Cryptographie</b>	Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques		✓	✓	✓
<b>Pare-feu</b>	Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement	✓		✓	
<b>Contrôles d'accès logiques</b>	Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dûment habilitées		✓	✓	✓
<b>Sécurité physique des équipements et locaux</b>	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.	✓	✓	✓	



# Cybersécurité

## Capacité d'audit

Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I.

## Cluses contractuelles avec les partenaires

Mécanismes organisationnels destinés à s'assurer que les partenaires et prestataires mettent en œuvre les mesures nécessaires pour ne pas impacter la sécurité des S.I. de leurs clients

## Formation et sensibilisation

Mécanismes organisationnels dont l'objectif est d'expliquer aux utilisateurs, administrateurs, techniciens, PDG, clients, grand public, etc. en quoi leurs actions affectent la sécurité des S.I. Diffusion des bonnes pratiques de sécurité. Le cours actuel en est une illustration !

**D I C P**

✓ ✓ ✓ ✓

✓ ✓ ✓ ✓

✓ ✓ ✓ ✓



# Introduction

- › Définitions de la donnée
- › Cybersécurité, qu'est ce que c'est ?
- › Les menaces qui peuvent affecter les données
- › Quelques solutions et outils
- › Conclusion



# Les menaces

## › Quelques exemples d'attaques



Derniers articles | Archives | Recherche

### Copé, Hortefaux, Dassault... leurs messageries Orange piratées

par Emilien Ercolani, le 07 mai 2013 15:04 ★★★★★

Les messageries des téléphones portables de plusieurs personnalités politiques (JF Copé, B Hortefaux) ou industrielles (la famille Dassault) ont été piratées plusieurs semaines durant. Des plaintes ont été déposées, alors qu'Orange a lancé une enquête interne.

Publié le 13 avril 2014 à 12h24 | Mis à jour le 13 avril 2014 à 12h24

### Le centre allemand de recherche cible d'une cyberattaque

Agence France-Presse

Le centre allemand de recherche aéronautique et spatiale (DLR) a été la cible il y a quelques mois d'une cyberattaque présumée par un service de renseignements étranger, affirme le magazine Der Spiegel dimanche.

### Des machines à sous vidées à cause d'une faille informatique

Le Monde.fr | 15.04.2014 à 09h09 • Mis à jour le 15.04.2014 à 10h46

Abonnez-vous à partir de 1 € Réagir Classer Partager



Actualités > Société

### Une panne réseau a cloué au sol les avions d'American Airlines

Près de 670 vols ont été annulés hier, en raison d'un problème d'accès au système de réservation. La compagnie s'est appuyée sur les réseaux sociaux pour informer ses clients.

Gilbert Kallenborn, avec AFP | 01net | le 17/04/13 à 11h23 | laisser un avis  
Tweet +1

### Panne informatique à l'hôpital de

En l'espace de deux jours, mercredi et jeudi, l'accueil aux urgences de a été très perturbé. Il a fallu diriger les patients vers d'autres hôpitaux.

Publié le 10.01.2009

### Ukraine : le mystérieux virus Snake infecte les ordinateurs du gouvernement

Publié le 08.03.2014, 16h50 | Mise à jour : 17h23

Recommander 52 personnes le recommandent. Inscription pour Twitter 64 +1 Share



Illustration. Un mystérieux virus a été réactivée ces derniers jours et vise les ordinateurs ukrainiens. | LP/ Olivier Arandel



# Les menaces



## › Quelques exemples d'attaques



### Bug informatique à La Poste : "Tout est rentré dans l'ordre"

par Caroline Piquet  
le 30 juillet 2013 à 15h50, mis à jour le 30 juillet 2013 à 18h59.

**A la suite d'une panne informatique, les opérations de prélèvements et de virements bancaires accusent un retard de 24 heures. Ce mardi, les clients ne pouvaient accéder à leurs soldes sur Internet et il leur était impossible de retirer de l'argent aux distributeurs automatiques.**

Help! My fridge is full of spam and so is my router, set-top box and console  
Security company says it discovered spam and phishing campaign run over Christmas, which involved internet fridge

### Gibraltar: un incendie interrompt des services de paris en ligne

AFP, 20/04 23:31 CET



### Hacker un pacemaker, c'est possible et c'est dangereux

10:12 - vendredi 19 octobre 2012 - Par Johann Mise - Source : France Info



### Une panne informatique paralyse Wall Street pendant 3 heures

Edité par MYTF1News avec AFP  
le 23 août 2013 à 06h50, mis à jour le 23 août 2013 à 07h02.

Charles Arthur  
Follow @charlesarthur Follow @guardiantech  
theguardian.com, Tuesday 21 January 2014 11.40 GMT  
Jump to comments (19)



### Un avion espion « plante » le système informatique d'un aéroport

Par Pierre Dandumont 5 MAI 2014 12:30 - Source: NBC News | 0 COMMENTAIRE



# Les menaces

The timeline features a central horizontal blue line with four square markers. Above the line, from left to right: 1. A photograph of three industrial cooling towers with white steam rising against a blue sky. 2. A photograph of a person in a purple shirt sitting at a desk with multiple laptops, looking distressed with their hand to their face. A red 'RANSOMWARE' sign is visible on the wall behind them. 3. A photograph of a hand holding a smartphone displaying a mobile banking app interface with various account balances. Below the line, from left to right: 1. A photograph of a large black oil tanker ship sailing on the open sea. 2. A dark background with faint, glowing blue binary code (0s and 1s) scattered across it.

**JUN 2009**  
Tout le secteur pétrolier iranien est paralysé par **une attaque informatique.**

**23 AVRIL 2012**  
Un virus met en panne toutes les centrifugeuses des usines atomiques iraniennes.

**FIN AOÛT 2013**  
Neuf fois plus de virus sur les applications bancaires des téléphones portables que l'année précédente.

**2014**  
Le réseau internet de la Chine est inaccessible pendant plusieurs jours. Les autorités reconnaissent avoir subi « LA PLUS GRANDE ATTAQUE INFORMATIQUE DE LEUR HISTOIRE ».

Source leMag' 2/10/2017

# Les menaces



Source leMag' 2/10/2017

LA SÉCURISATION DES DONNÉES (ACCÈS, SAUVEGARDE, ARCHIVAGE...)



# Les menaces

- › Destruction/altération accidentelle
  - Panne de matériel
  - Mauvaise manipulation
- › Destruction/altération malveillante
  - Virus, cryptolocker, ransomware...
  - Piratage, fraude interne...
  - Vol

# Les menaces

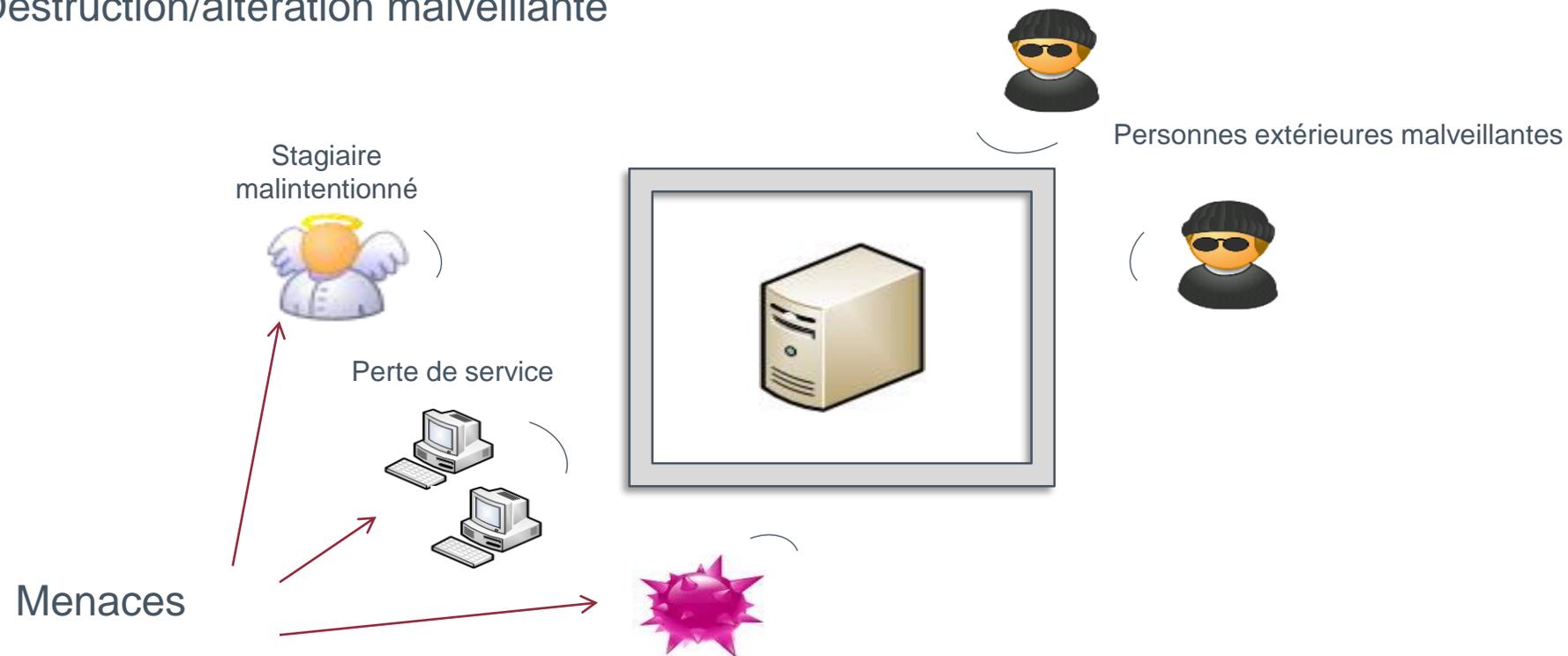
- › Destruction/altération accidentelle
  - Panne de matériel
- › Comment s'en prémunir ?
  - Mettre en place une stratégie de sauvegarde
  - Utiliser des technologies tolérant les pannes (système RAID)
  - Dupliquer les données sur des périphériques différents (Serveurs de stockage, disque local...)
  - Ne pas stocker de données sur des clefs USB...

# Les menaces

- › Destruction/altération accidentelle
  - Mauvaise manipulation
- › Comment s'en prémunir ?
  - Vérifier les privilèges du compte utilisateur
  - Mettre en place une stratégie de sauvegarde
  - Dupliquer les données sur des périphériques différents (Serveurs de stockage, disque local...)

# Les menaces

## Destruction/altération malveillante



# Les menaces

- › Destruction/altération malveillante
  - Virus, cryptolocker, ransomware...
- › Comment s'en prémunir ?
  - Installation des mises à jour système
  - Installation d'un logiciel Antivirus et ses mises à jour (au moins une fois par jour)
  - Vérifier les privilèges du compte utilisateur
  - Sensibiliser les utilisateurs
  - Mettre en place une stratégie de sauvegarde
  - Dupliquer les données sur des périphériques différents (Serveurs de stockage, disque local...)

# Les menaces

- › Destruction/altération malveillante
  - Piratage, fraude interne...
- › Comment s'en prémunir ?
  - Installation des mises à jour système
  - Installation d'un logiciel Antivirus et ses mises à jour (au moins une fois par jour)
  - Vérifier les privilèges du compte utilisateur
  - Vérifier les droits d'accès aux fichiers/répertoires
  - Mettre en place une stratégie de sauvegarde
  - Dupliquer les données sur des périphériques différents (Serveurs de stockage, disque local...)

# Les menaces

- › Destruction/altération malveillante
  - Vol
- › Comment s'en prémunir ?
  - Mettre en place une stratégie de sauvegarde
  - Dupliquer les données sur des périphériques différents (Serveurs de stockage, disque local...)
  - Mettre en place le chiffrement des données
  - Protéger le matériel (câble antivol, plaquette d'identification antieffraction...)



# Introduction

- › Définitions de la donnée
- › Cybersécurité, qu'est ce que c'est ?
- › Les menaces qui peuvent affecter les données
- › **Quelques solutions et outils**
- › Conclusion



# Quelques solutions

- › Outils pour la copie automatique :
  - Rsync (Linux, MACOSX)
  - SyncToy (Microsoft Windows)
- › Outils pour la sauvegarde
  - Bacula serveur (Linux)
  - Bacula client (Linux, MACOSX, MS Windows)



# Quelques solutions

## › Au CERMAV :

- Mode opératoire pour la sauvegarde et l'archivage des données
- Mode opératoire pour la configuration de SyncToy

<i>Système d'Organisation de l'Unité de Recherche CERMAV</i>	<i>Mode Opératoire</i>	<b>MO-13-030</b>
<b>CERMAV</b>	<b>SAUVEGARDE ET ARCHIVAGE DES DONNEES</b>	indice page F 1/4

### OBJET :

Ce mode opératoire décrit les modalités de sauvegarde et d'archivage des données au sein du laboratoire et préconise une structuration des données de façon à assurer leur pérennité.

### DOMAINE D'APPLICATION :

Ensemble du personnel du CERMAV

### VOCABULAIRE :

### DIFFUSION :

SOURCE

### DOCUMENTS DE REFERENCE :

Bureautique : Configuration de SyncToy (MO-13-066)

Comptes rendus conseil de laboratoire

Feuille de route du doctorant (FO-12-005)

Programme de séjour postdoctoral (MO-12-027)

# Quelques solutions

## › Chiffrement

- Bitlocker (Microsoft Windows)
- FileVault (MAC OSX)
- Veracrypt (Linux)

## › Modification des droits

- Cacls et onglet sécurité des dossiers/fichiers (Microsoft Windows)
- Chmod et chown (MACOSX, Linux)

Format rwx	Format Binaire	Format Décimal
---	000	0
—x	001	1
-w-	010	2
-wx	011	3
r—	100	4
r-x	101	5
rw-	110	6
rwX	111	7

# Quelques solutions

- › Protection contre les intrusions réseau
  - **Ne pas autoriser l'accès au réseau Internet** depuis les machines d'acquisition et réciproquement les **machines ne doivent pas être accessibles depuis le réseau Internet.**
  - Activer le pare-feu de l'ordinateur
    - › Pare-feu Windows
    - › Coupe-feu MAC OSX
    - › Iptables Linux
  - Placer ou faire placer les machines d'acquisition dans un réseau dédié (VLAN)



# Introduction

- › Définitions de la donnée
- › Cybersécurité, qu'est ce que c'est ?
- › Les menaces qui peuvent affecter les données
- › Quelques solutions et outils
- › **Conclusion**



# Conclusion

- › La protection du patrimoine scientifique et technique est l'affaire de tous
- › Ne se limite pas à des mesures techniques
- › Questions ?