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

Cyril Bras 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

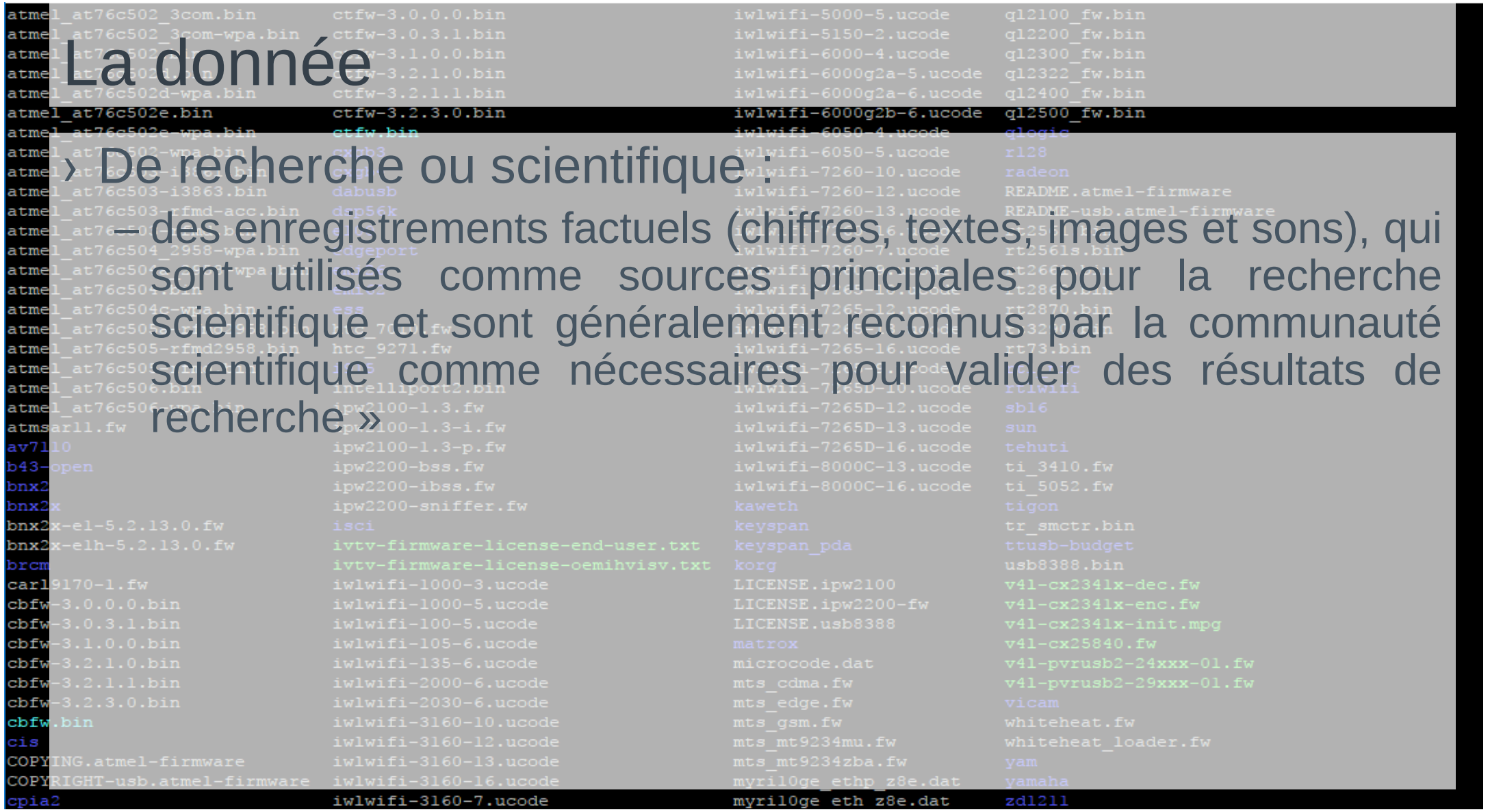
› Définition générale :

– 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.

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 »



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 :

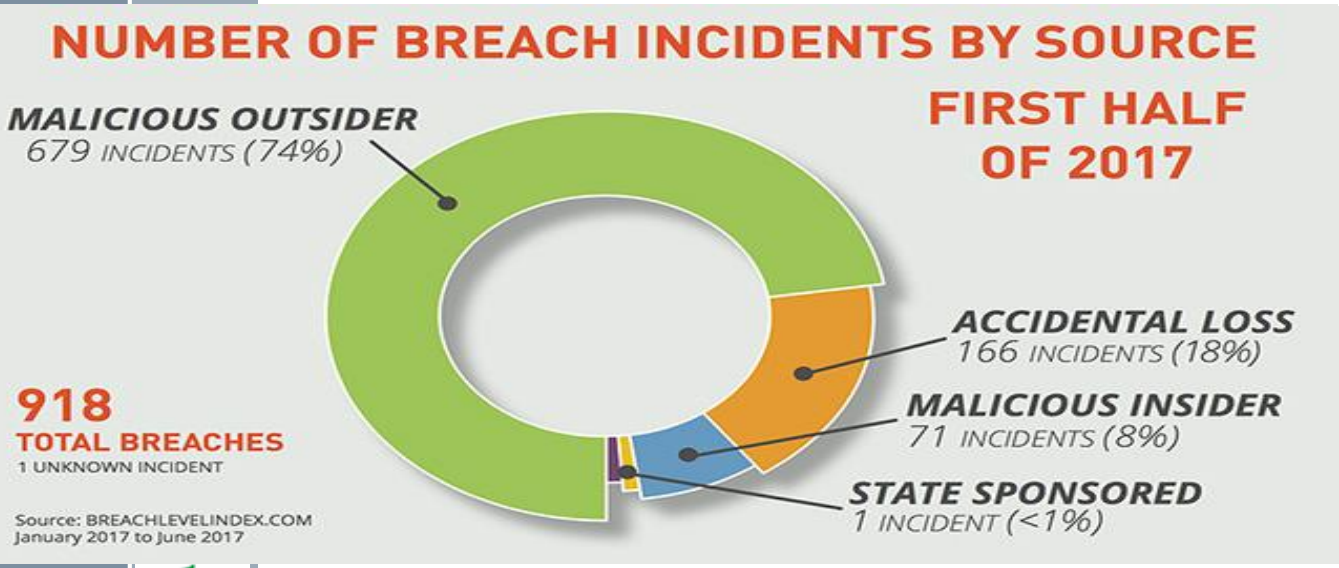
– On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour **protéger le cyberenvironnement et les actifs 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.

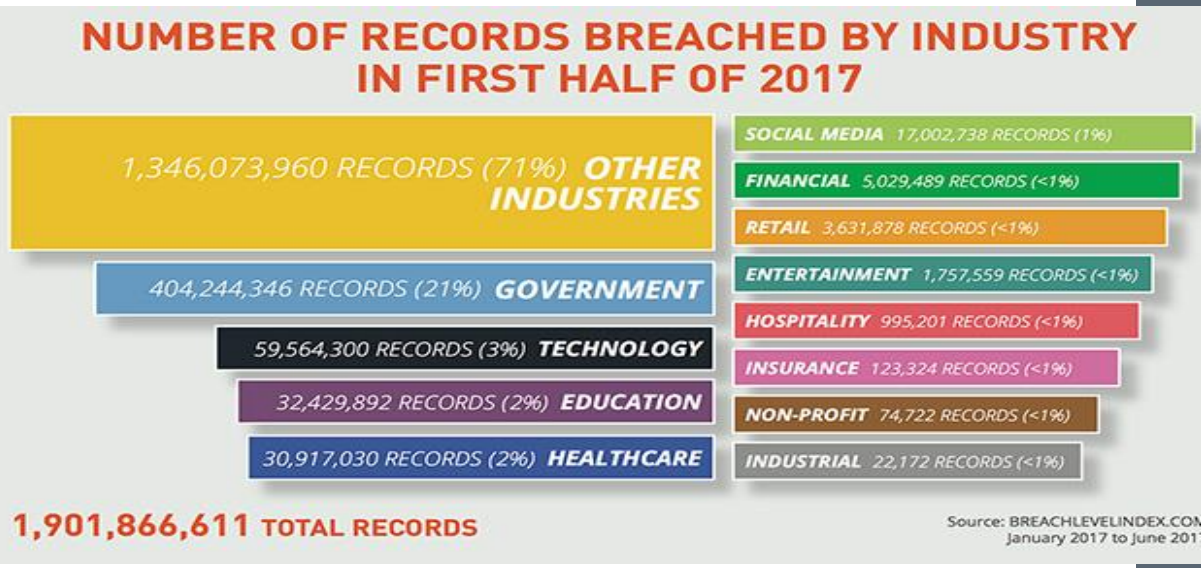
Cybersécurité

› 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



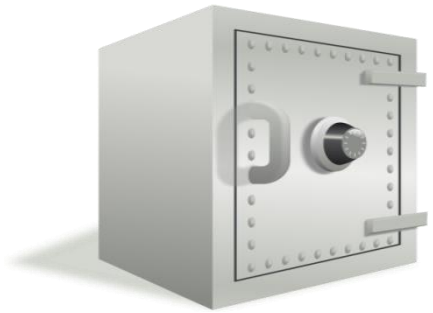


Cybersécurité

› 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…

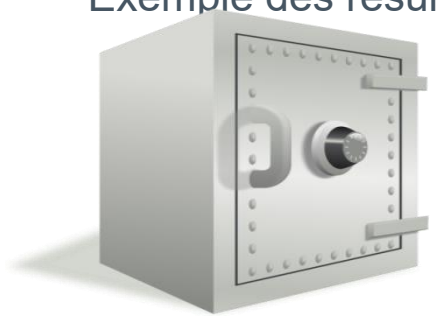
Cybersécurité

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

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

Cybersécurité

		D	I	C	P
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.	✓	✓	✓	✓
Clauses 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 !	✓	✓	✓	✓

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, Hortefeux, 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 Hortefeux) 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.

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 5

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

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

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 voir ce que vos amis recommandent. | Tweeter 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.

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

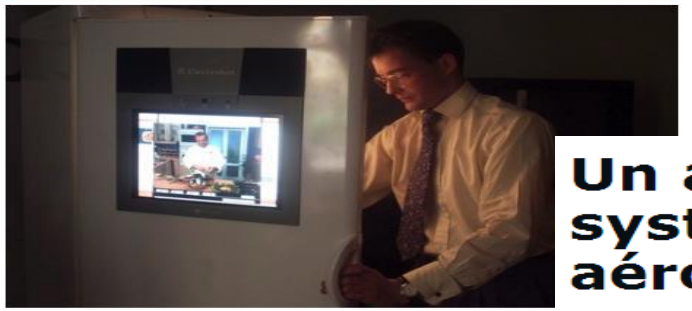
10:12 - vendredi 19 octobre 2012 - Par Johann Mise - Source : France Info

Zoom

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

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



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.

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

Source leMag' 2/10/2017

Les menaces

Source leMag' 2/10/2017

Les menaces

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

Les menaces

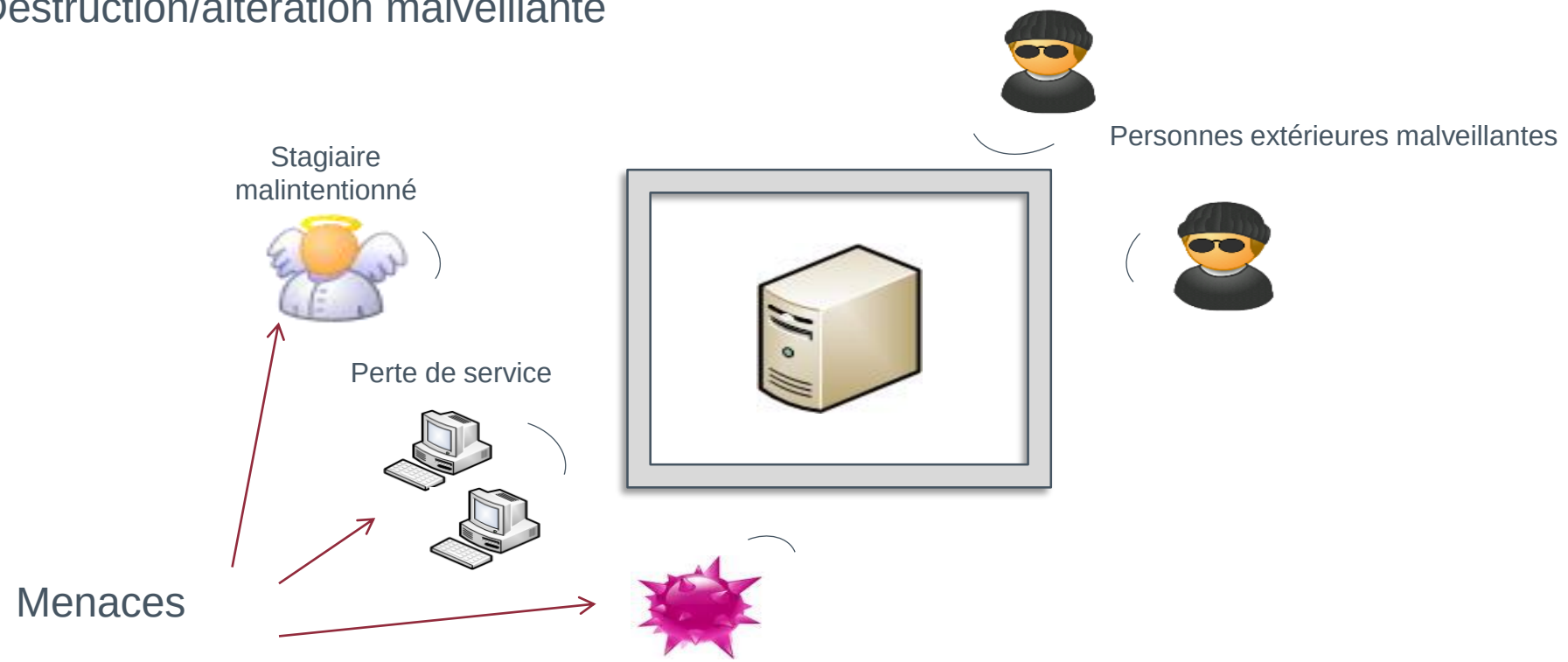
- Destruction/altération accidentelle
  - Panne de matériel
- Comment s'en prémunir ?
  - Mettre en place une stratégie de sauvegarde
  - Utiliser des technologies tolérant les pannes (système RAID)
  - Dupliquer les données sur des périphériques différents (Serveurs de stockage, disque local…)
  - Ne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

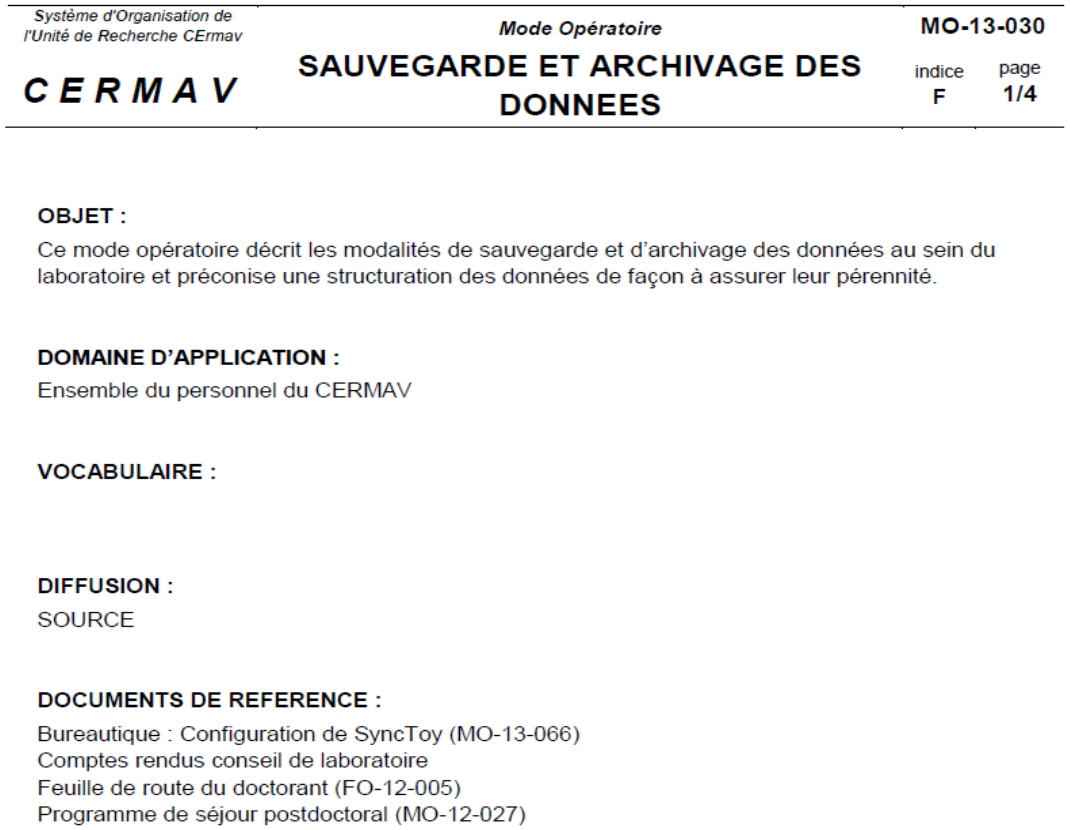
- Définitions de la donnée
- Cybersécurité, qu'est ce que c'est ?
- Les menaces qui peuvent affecter les données
- Quelques solutions et outils
- Conclusion

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



Système d'Organisation de l'Unité de Recherche CErmav	Mode Opératoire	MO-13-030
C E R M A V	SAUVEGARDE ET ARCHIVAGE DES DONNEES	indice F / page 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 ?