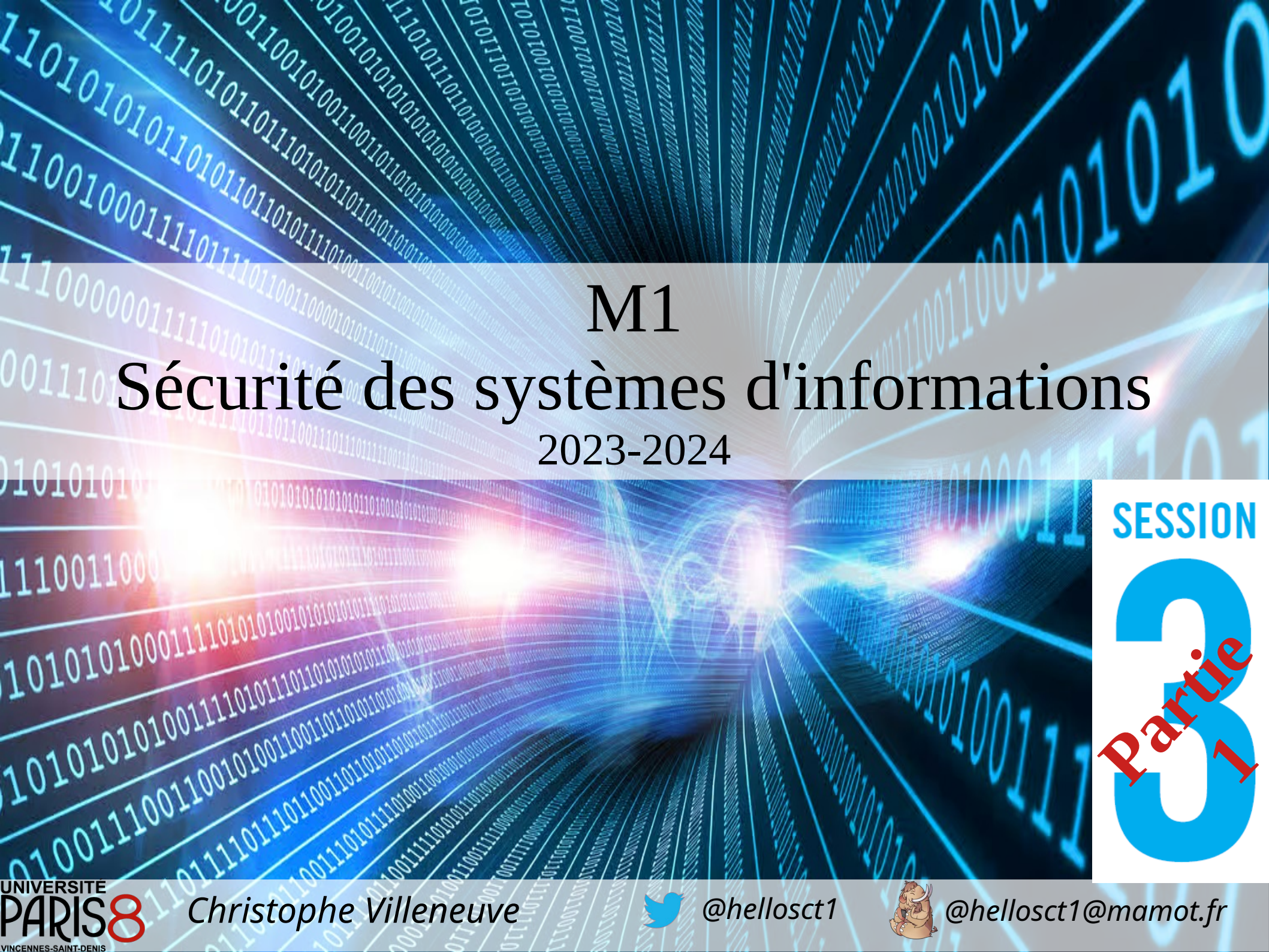


# M1
# Sécurité des systèmes d'informations
2023-2024

SESSION 3
Partie 1

UNIVERSITE PARIS 8 VINCENNES-SAINT-DENIS
Christophe Villeneuve @hellosct1 @hellosct1@mamot.fr

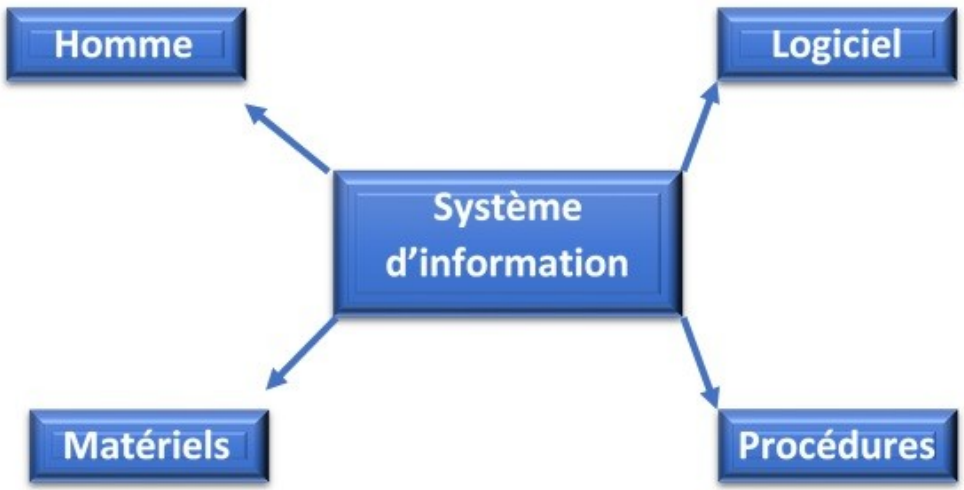
# Aujourd’hui : Session 3 : Hygiène numérique

- Correction TP 2
- Connaître le Système d’Information
- Maitriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.
- Nomade

- Connaître le Système d’Information
- Maitriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.
- Nomade

# Correction TP 2

- Sujet :
  - Si vous étiez victime d'une attaque cybercriminelle, quelles pourraient être les conséquences (impacts) sur votre vie privée ?
- Réponse : Session 2 (partie 1) - slide 62 et +
  - Gains financiers
  - Utilisation de ressources
  - Chantage
  - Espionnage

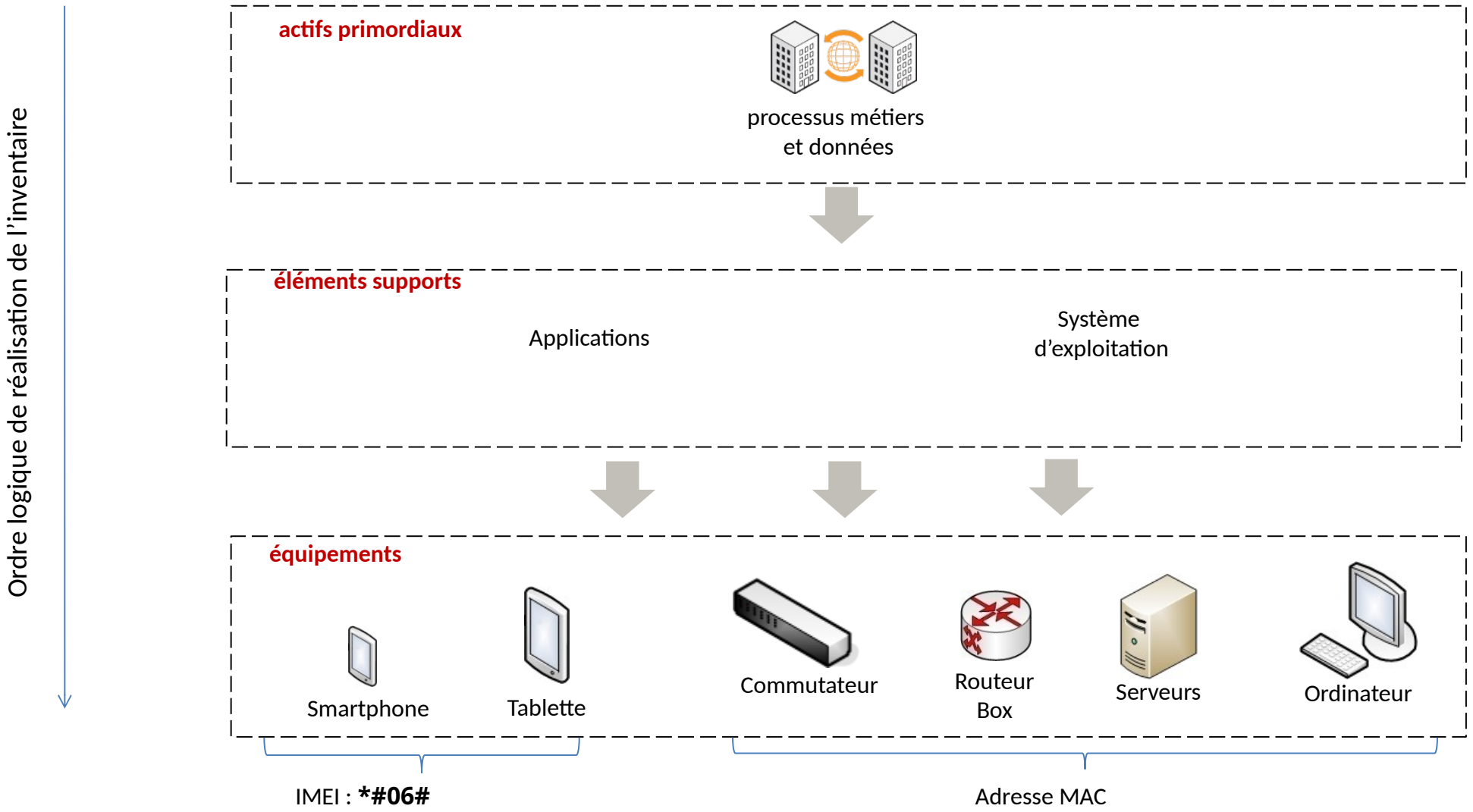



- Connaître le Système d'Information
- Maitriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.

# Identifier les composants du S.I.

- Au-delà des connaissances des composants :
  - L'inventaire permettra de mieux déterminer
    - Les menaces et les mesures de protection applicables.
- Tout projet sécurité doit :
  - Intégrer forcément un inventaire des biens.
- L'inventaire des biens doit :
  - Suivre une méthodologie logique
    - afin d'être exhaustif
  - En commençant par l'inventaire des métiers.

# Comprendre l'identification des composants (1/2)



# Comprendre l’identification des composants (2/2)

- Les équipes opérationnelles
  - Administrateurs réseau
  - Sécurité et système
  - Chefs de projet
  - Développeurs / Développeuses
  - RSSI


- Ont des accès au système d’information

Risque :

- Par inadvertance
- par méconnaissance des conséquences de certaines pratiques

-> Réaliser des opérations génératrices de vulnérabilités

# Identifier les biens (pour l'inventaire) (1/2)

- Données sensibles :
  - Personnel
    - mots de passe,
    - cartes de crédit,
    - Documents personnels
    - Etc...
  - Entreprise
    - plan marketing
    - fichier client
    - Brevets
    - Contrats
    - Etc...

- Les applications

  + les versions :

  - Libre office
  - Office 20xx
  - Gimp
  - IDE
  - Navigateur web
  - Etc...

# Identifier les biens (pour l'inventaire) (2/2)

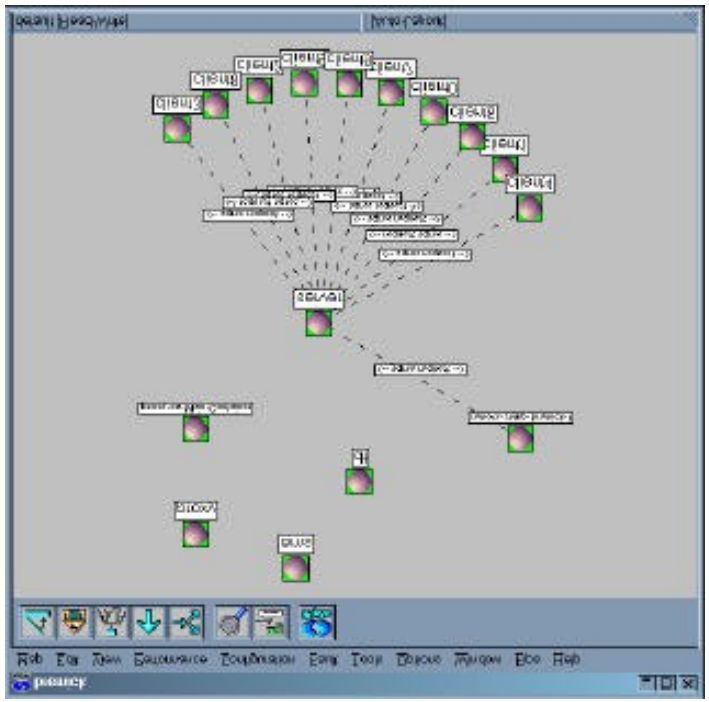
- Systèmes d'exploitations :
  - Android
  - IOS
  - Windows
  - Linux
  - MacOS
  - Etc...
- Equipements :
  - Ordinateur
  - Tablette
  - Téléphone
  - Serveur
  - Box
  - Routeur
  - Etc...

# Inventorier les biens

Outil d'identification

- Ordinateurs en réseau

HP OpenView servicenow



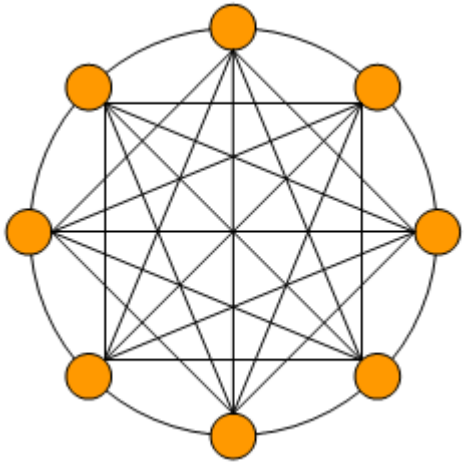
Outil d'identification

- Logiciels installés :
  - Ordinateur
  - Téléphone
- Les versions
  - Ex : Diagnostiques


# Types de réseau

- BAN (Body Area Network)
  - Réseau composé de télé transmetteur utilisé dans le domaine de la santé
- PAN (Personal Area Network)
  - Réseau centré autour d'une personne
    - interconnectant ordinateur, téléphone, tablette, voiture... (moins de 10m)
- WPAN (Wireless PAN)
  - Réseau PAN sans fil utilisant des technologies
    - IrDA, ZigBee, Bluetooth, Wireless USB
- LAN (Local Area Network)
  - Réseau local interconnectant plusieurs périphériques
    - permettant l'échange d'informations entre plusieurs individus
- MAN (Metropolitan Area Network)
  - Réseau plus large qu'un LAN et étendu par exemple sur une ville
- CAN (Campus Area Network)
  - Réseau s'étendant sur plusieurs LAN, et de la taille d'une université
- WAN (Wide Area Network)
  - Réseau d'une étendue nationale ou internationale.
    - Exemple : Internet.

# Interconnexion



- Connaître et maîtriser les points d'interconnexion
  - Accès Internet via :
    - Box Internet (ADSL, Fibre, …) ;
    - téléphone/carte 3G/4G, etc.
  - Interconnexion avec d'autres réseaux
    - Ex : universités, partenaires, prestataires, etc
    - Liaison dédiée : E1/T1 carrier, fibre noire
    - Réseau privé virtuel (VPN) sur un WAN
      - appartenant à un opérateur ou sur Internet
    - Liaison satellite.

# A retenir

- Connaître son matériel
- Ne pas faire n’importe quoi avec les logiciels

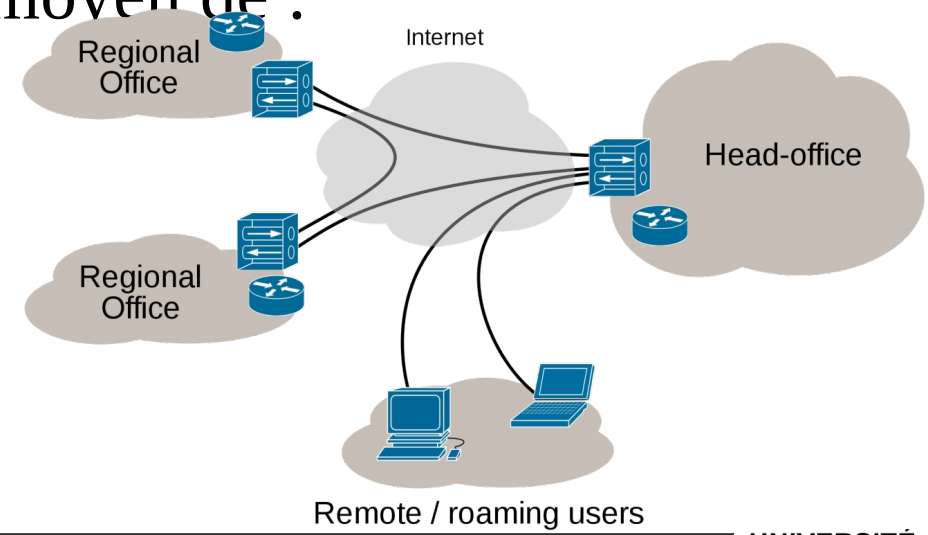

https://school.hello-design.fr

3A

- Connaître le Système d’Information
- Maitriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.
- Nomade

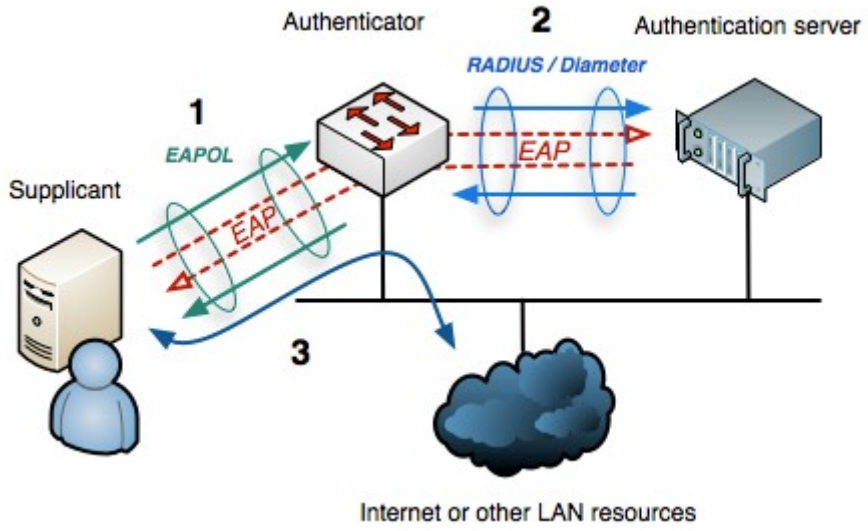
# Sécuriser le réseau interne (1/2)

- Créer des zones dans le réseau interne
  - Zones distinctes pour les serveurs, postes de travail, visiteurs
  - Assurer la confiance par l'authentification mutuelle des composants :
    - chaque composant s'authentifie avant le début de l'échange
    - permet d'éviter l'usurpation d'identité
  - Assurer le cloisonnement au moyen de :
    - VLAN, VRF, sous-réseaux
    - Ne pas oublier d'implémenter un mécanisme de filtrage !



# Sécuriser le réseau interne (2/2)

- Restreindre les accès aux réseaux internes
  - 802.1X permet de contrôler l'accès réseau
    - de s'assurer que l'autorisation
    - n'est accordé qu'après authentification de l'utilisateur ;
  - Recourir à l'authentification avant d'autoriser l'accès au réseau :
    - l'authentification peut se faire par l'usage d'un certificat ou d'une carte à puce ;
    - l'authentification est centralisée sur un serveur qui donne les accès en fonction de l'identité de l'utilisateur (Exemple : Serveur Radius).



# BYOD

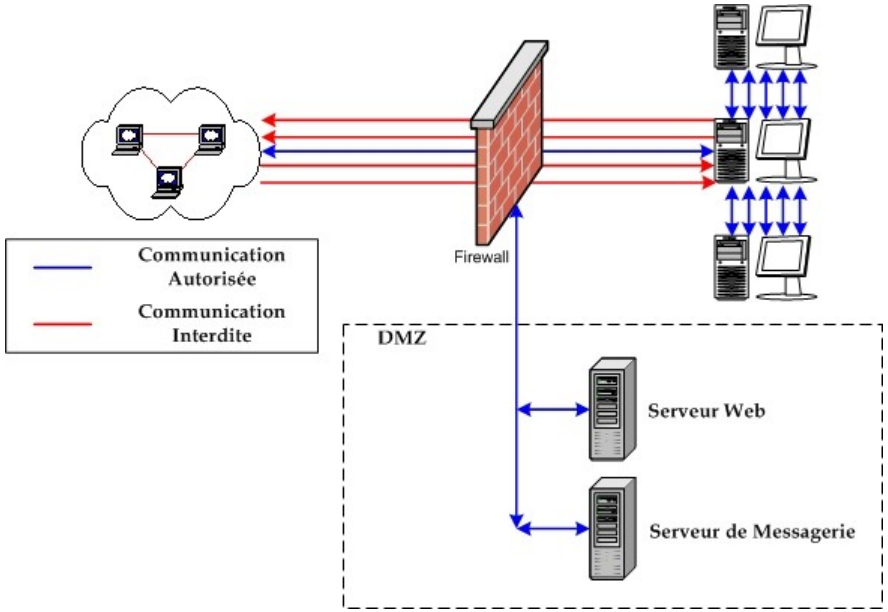

- Réseau permet de partager des informations,
  - Risque aussi de propager les infections de codes malveillants.
- Les terminaux personnels
  - n’ont pas le même niveau de sécurité que les terminaux de l’entreprise / université :
    - Sur un terminal personnel :
      - Un utilisateur installe les logiciels de son choix, avec la configuration de son choix. L’antivirus n’est pas forcément à jour
    - Sur un terminal professionnel
      - Les logiciels sont installés de manière centralisée, et les sources vérifiées
- Les terminaux personnels sont connus :
  - Pour être une source de fuite de données sensibles pour l’entreprise

Volontaire ou pas

*Le S.I. est un tout, un maillon faible affaiblir tout l’ensemble.*

# Contrôler les échanges internes (1/2)

- Filtrer les flux pouvant être échangés entre les zones :
  - identifier les ports réseau utiles ;
  - identifier les protocoles réseau autorisés ;
  - disposer d'une matrice de flux indiquant les flux autorisés et interdits entre les zones.

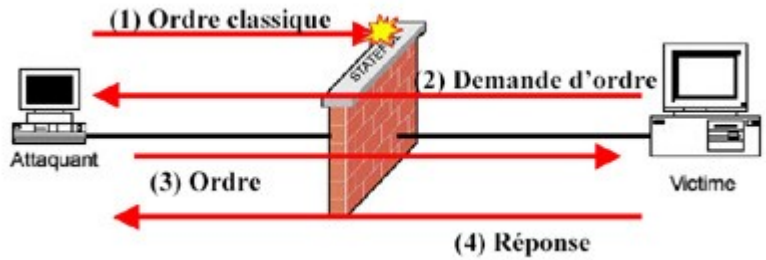


# Contrôler les échanges internes (2/2)

- Autoriser explicitement
  - Les adresses IP (machines) d'une zone

    à échanger avec les adresses IP (machines)

    d'une autre zone
- Liste blanche
  - Définir les adresses IP pour les échanges
    - Et non pas une liste noire.
    - Une liste noire ne peut en effet jamais être exhaustive, et est forcément d'un intérêt limité.

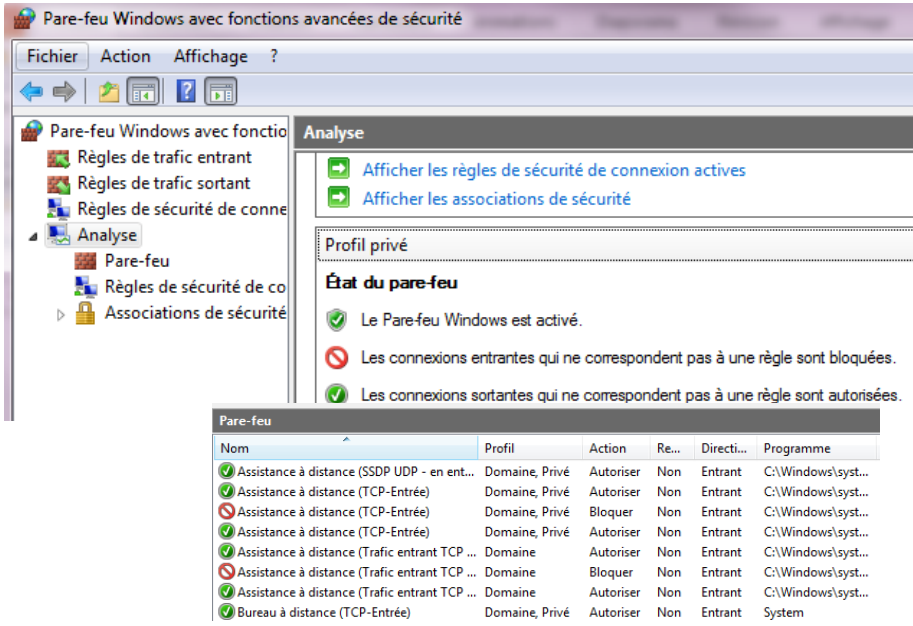



Appliquer le principe « Tout ce qui n'est explicitement autorisé est interdit » lors de la gestion des flux.

# Protéger le réseau interne d'Internet

- Le réseau interne est à protéger
  - Il est considéré comme 'de confiance'
- Les équipements interagissant avec Internet peuvent être
  - placés dans une zone spéciale appelée '**Zone Démilitarisée (DMZ)**'
    - avec un niveau de filtrage et de contrôle plus accru que le réseau interne.
- protégés d'Internet par des « pare-feux » filtrant les échanges de flux
    - Équipement dédié protégeant le réseau ou logiciel « pare-feu personnel »

- Sous Windows,
  utiliser le pare-feu par défaut ou un pare-feu tiers
  . Ex : Zone Alarm, simpleWall,...
- Toujours contrôler les connexions entrantes ;
- Autoriser les applications au travers du pare-feu, au cas par cas



# Accès distant

- Il est possible d’accéder à distance à un réseau pour faire :
  - du télétravail ;
  - de la téléassistance ;
  - de la téléadministration.

- Il est recommandé d’avoir
  - des points d’entrée identifiés pour les accès distants :
    - Serveurs d’authentification : TACACS+, RADIUS ;
    - Concentrateurs VPN ;
    - Remote Access Server (RAS).

# Accès distant

- Les moyens sécurisés pour les accès distants :
  - **SSH** au lieu de telnet
    - pour l'établissement de connexion à distance sur un équipement
  - Secure remote desktop
    - pour la prise en main à distance d'un bureau
  - **SFTP** ou **SCP**
    - pour la copie distante
  - **HTTPS**
    - pour l'accès à une interface Web
      - Exemple : Teamviewer, RustDesk, TightVNC...
  - Réseau Privé Virtuel (**VPN**) établit sur un réseau (Non contrôlé)
    - VPN IPSEC : permet l'authentification et le chiffrement. Il est utilisé pour protéger le trafic réseau ;
    - VPN SSL : protège essentiellement le trafic Web, et est facile à déployer.

# Sécuriser l’administration (1/3)

- Restreindre/Interdire

  les interfaces d’administration depuis Internet

L’administration d’un composant
ne doit pouvoir se faire que
depuis le réseau interne

Ouvrir un accès VPN
en cas de nécessité d’accéder à distance

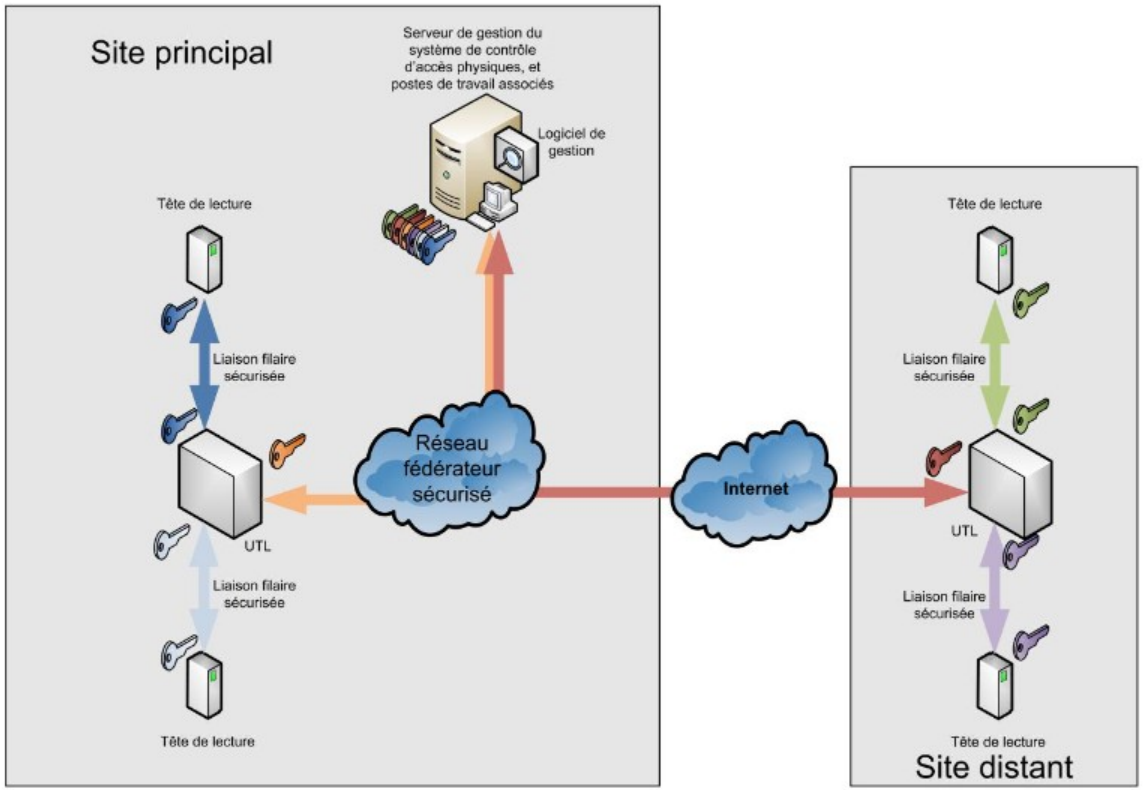



*Figure 4 : exemple d'un système de contrôle d'accès sans contact*

https://www.ssi.gouv.fr/uploads/IMG/pdf/Securite_des_technologies_sans_contact_pour_le_controle_des_acces_physiques.pdf

# Sécuriser l’administration (2/3)

- Restreindre les accès aux interfaces d’administration sur les sites Web

Pour des sites web développés avec :

- CMS (Content Management System)
  - Drupal, Joomla, Wordpress...
- Framework
  - Symfony, Django...

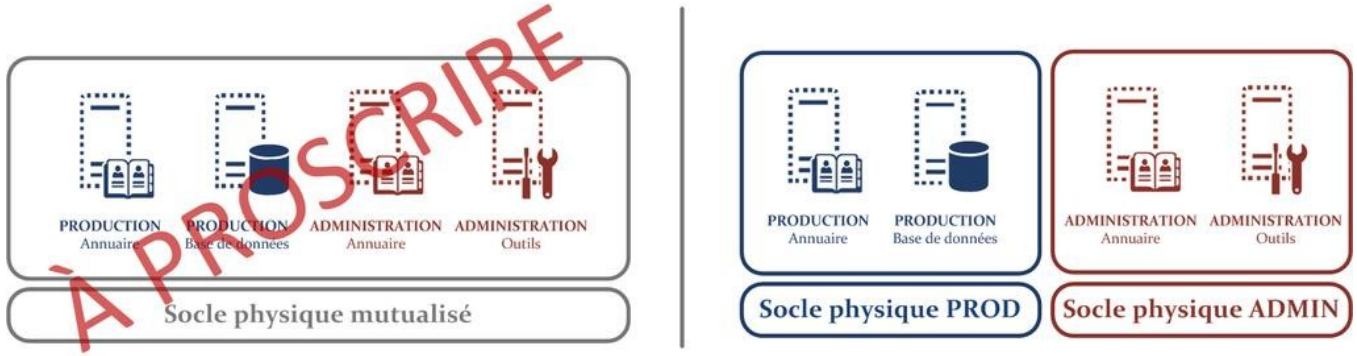
- Le lien de la page d’administration peut être facilement trouvé (sauf à la modifier)

- Des attaques en « brute force » peuvent être menées pour deviner le mot de passe administrateur ;

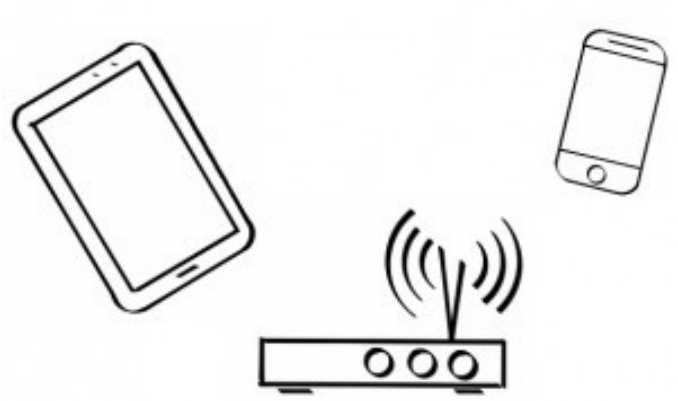
- Modifier le compte « admin » par défaut.

# Sécuriser l’administration (2/3)

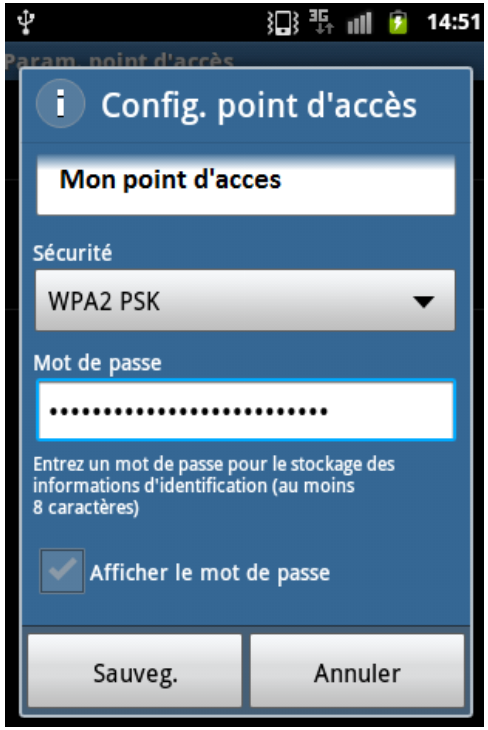
- Utiliser un réseau d’administration dédié :
  - Ce réseau doit être séparé
    - Du réseau de production de manière
    - Seul les postes autorisés peuvent s’y connecter
  - Avoir une liste blanche des administrateurs
    - Autorisés à se connecter à ce réseau ;
  - Authentifier mutuellement :
    - Les postes des administrateurs
    - Les équipements à administrer.



# Wifi : son réseau (1/2)



- Pour sécuriser son réseau Wifi :
  - Protéger la confidentialité des communications en effectuant un chiffrement à l'aide d'une clé :
    - La clé doit être composée de plusieurs caractères, alphanumérique (au moins 15).
  - Choisir la technologie la plus élevé
    - WPA2 (Wi-Fi Protected Access 2)
  - Choisir l'algorithme de chiffrement
    - CCMP (Counter Cipher Mode Protocol )
  - Modifier le SSID
    - nom du réseau Wifi fourni
  - Modifier les identifiants fournis par défaut
    - pour accéder à l'interface d'administration :
    - En général, sur les box, saisir l'url :
      - http:192.168.1.1 ou http:192.168.1.254 ou ….
      - pour atteindre l'interface d'administration.
  - Ne pas divulguer protéger sa clé WIFI.



# Wifi : son réseau (2/2)


- WPS = Wi-Fi Protected Setup
  - Disponible pour certaines box internet
    - Reconnu vulnérable à une attaque

      par force brute sur le code PIN.
    - Sur les box internet,
      - il est donc préférable de configurer la connexion Wi-Fi manuellement
      - Choisir son propre mot de passe (robuste) ;
  - Important
    - Cocher l'option qui permet de désactiver automatiquement le WPS au-delà de 5 tentatives de clé

# Wifi : Wifi privé vs Wifi public (1/2)

- Le Wifi privé
  - Quand :
    - Pour un réseau interne
    - Pour donner l'accès à des personnes de confiance.
  - Dans un LAN,
    - Utilisation possible comme moyen d'interconnexion

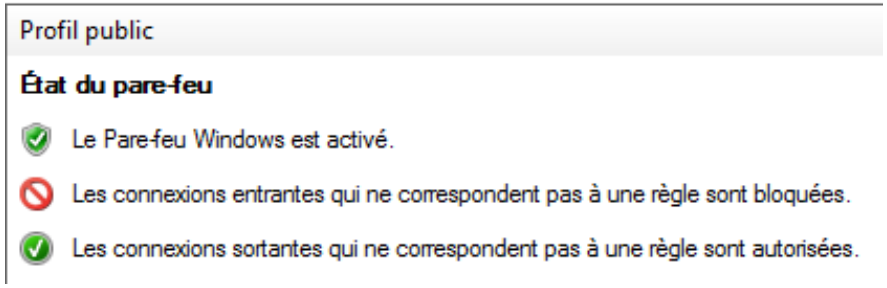
      → On parle alors de WLAN
    - Pour ces wifi en entreprise
      - Mettre en place si possible une authentification par certificats
      - Evite que tous les utilisateurs partagent le même mot de passe.

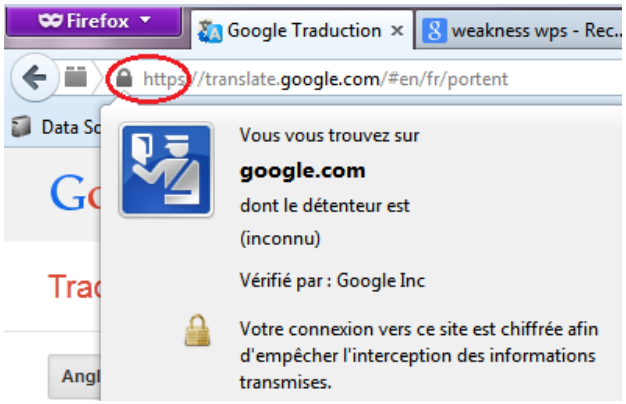
# Wifi : Wifi privé vs Wifi public (2/2)

- Le Wifi public : appelé hotspot
  - Fourni aux personnes
    - De non confiance
    - Au grand public
  - Souvent fourni pour un accès Internet unique
    - Hotspot Wifi : Wifi dans les aéroports, McDonald...
  - Ne pas oublier que tous les utilisateurs connectés sur le même hotspot
    - peuvent écouter toutes les conversations
      - Sauf si la page WEB visitée est en HTTPS)

# Wifi Public : Bonnes pratiques

- Désactiver les options de partage :
  - Arrêter la découverte réseau
  - Arrêter le partage de fichiers et d'imprimantes
  - Activer le pare-feu du poste
- Sous Windows
  - un pare-feu existe par défaut :
    - Contrôler les connexions entrantes si possible
    - Les connexions sortantes




Si cela est possible, utiliser un VPN sur un Wifi public.

# A retenir

- Un réseau par services d’entreprise
- Un réseau dédié vers les serveurs
  - Dev / Recette / PreProd / prod


https://school.hello-design.fr

3B

- Connaître le Système d'Information
- Maitriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.
- Nomade

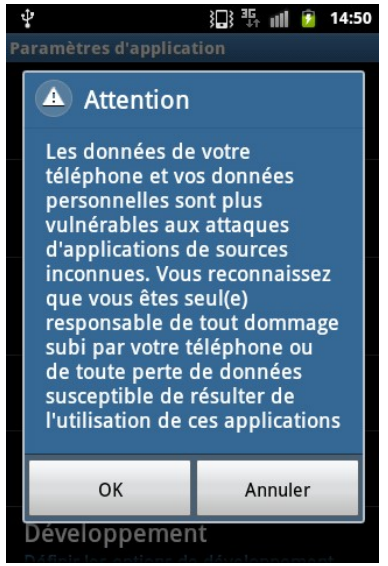
# Choisir les applications (1/2)

Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?

- On ne connaît pas forcément
  - ni l'auteur,
  - ni le site hébergeant ce logiciel ;
- Certains escrocs sont spécialisés
  - Dans la fourniture de chevaux de Troie (malware)
    - Un malware est fourni avec le logiciel

Objectif peut être de récupérer

- Login
- mot de passe
- numéro de carte bancaire.

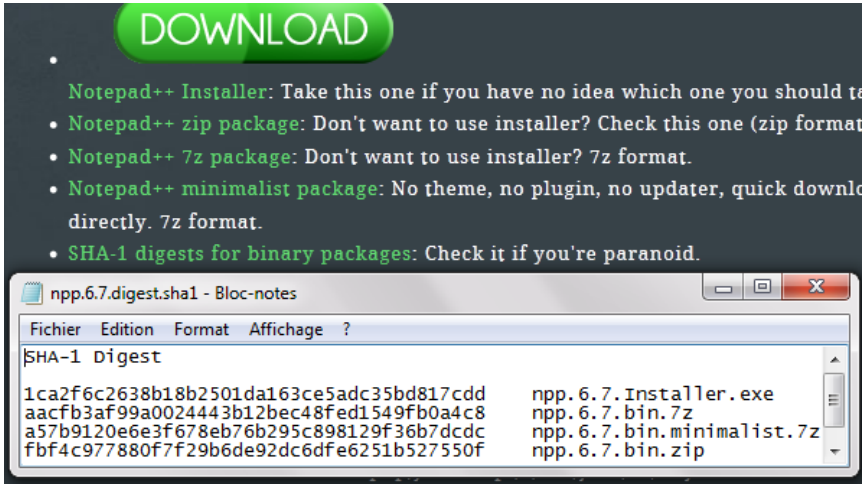



# Choisir les applications (2/2)

- Comment choisir :
  - Préférer des sources « sûres »
  - Utiliser des sources « de confiance » pour télécharger les logiciels ;
  - Sous Android :
    - interdire le téléchargement d’application depuis des sources inconnues.
  - utiliser les sites officiels (site de l’éditeur) pour les téléchargements.

# Logiciel : Vérifier la signature

- Recalculer la signature du fichier téléchargé
  - Avec la signature (checksum) indiquée sur le site
  - Et comparer.
-




# Applications payantes : N° série

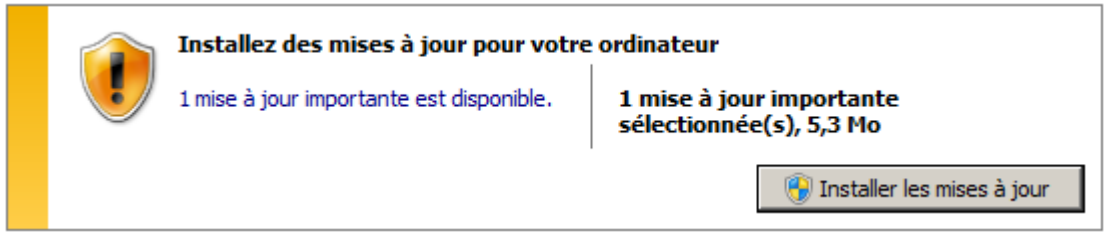
- Générateur de numéros de série (keygen)
  - Clés gratuites
  - Crack de logiciels
- Attention :
  - Les sites dédiés proposant cela sont souvent truffés de logiciels malveillants ;
  - Les versions « crackées » de logiciels
    - contiennent souvent

      des logiciels malveillants.

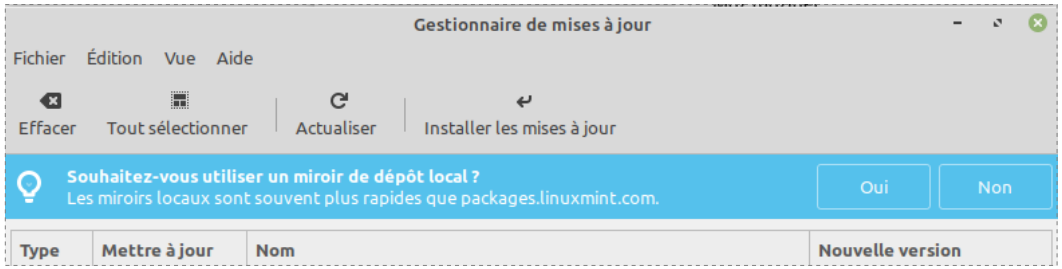
# Mises à jour des logicielles et systèmes (1/3)

- Rôle
  - Apporter des corrections à un(e) logiciel/application
    afin de corriger un dysfonctionnement ou une vulnérabilité
- Les mises à jour s'appliquent :
  - aux applications, aux systèmes d'exploitation, etc...

Windows




Linux




Mac

# Mises à jour logicielles et systèmes (2/3)

- En entreprise,
  - Les mises à jour s’effectuent de manière centralisée
  - Téléchargement sur des serveurs dédiés
    - Ex : serveur WSUS (Windows Server Update Services) pour Windows ;
  - Déploiement et observation sur des machines de test ;
  - Sauvegarde des machines de production ;
  - Déploiement sur les machines de production.

# Mises à jour logicielles et systèmes (3/3)

- Les mises à jour concernent
  - Le système d'exploitation
  - Tous les logiciels
- Important de faire les mises à jour régulièrement également
- Cycle de mises à jour régulières
- La plupart des logiciels ont une option
  - Menu : Mise à jour automatique
  - Il est recommandé de l'activer

Attention en entreprise:
C'est à l'administrateur de planifier et valider les mises à jour
→ cela inclut notamment des tests préalables de non régression

# Politique de mise à jour


- Nouvelle :
  - Failles → régulièrement découvertes
    - Systemes et/ou logiciels
  - Méthodes pour réussir son intrusion dans le SI
- Rester informé et appliquer les correctifs de sécurité
- Les actions de la politique de mise à jour :
  - Manière dont l'inventaire des composants du système d'information est réalisé
  - Sources d'information relatives à la publication des mises à jour
  - Outils pour déployer les correctifs dans le parc
  - Qualification des correctifs et leur déploiement progressif sur le parc

# Obsolescence !!!

- composants obsolètes doivent être isolés du reste du système
- Recommandation
  - Au niveau réseau
  - Filtrage strict des flux
  - Les secrets d’authentification
  - Etc..

# Anticiper la fin de la maintenance

- Utilisation d’un système ou logiciel obsolète
- Augmente les possibilités d’attaque informatique
- Les précautions :
  - Etablir et tenir à jour un inventaire des systèmes et applications du SI
  - Choisir des solutions dont le support est assuré pour une durée correspondant à leur utilisation
  - Assurer un suivi des mises à jour et des dates de fin de support des logiciels
  - Maintenir un parc logiciel homogène
  - Limiter les adhérences logicielles
  - Inclure dans les contrats avec les prestataires et fournisseurs
  - Identifier les délais et ressources nécessaires

# CVE

- CVE = Common Vulnerabilities and Exposures
- Site répertoriant les failles connues
  - Liste des CVE
    - https://cve.mitre.org
  - Complétement pour les CVE
    - https://www.securityfocus.com
  - National vulnerability database USA
    - https://nvd.nist.gov
  - Open CVE
    - https://www.opencve.io

# CVE : Déroulement

- 1 personne ou un groupe de sécurité trouve une faille puis la soumet
- La faille est analysée, puis validée ou non
- Si la faille est confirmé,
  - la faille est associée à une ou plusieurs catégories
- On lui applique une note
  - via le CVSS (Common Vulnerability Scoring System)
- Souvent un POC (Proof of concept est publié)
  - Exemple : https://www.cvedetails.com/cve/CVE-2019-10673/

**- CVSS Scores & Vulnerability Types**

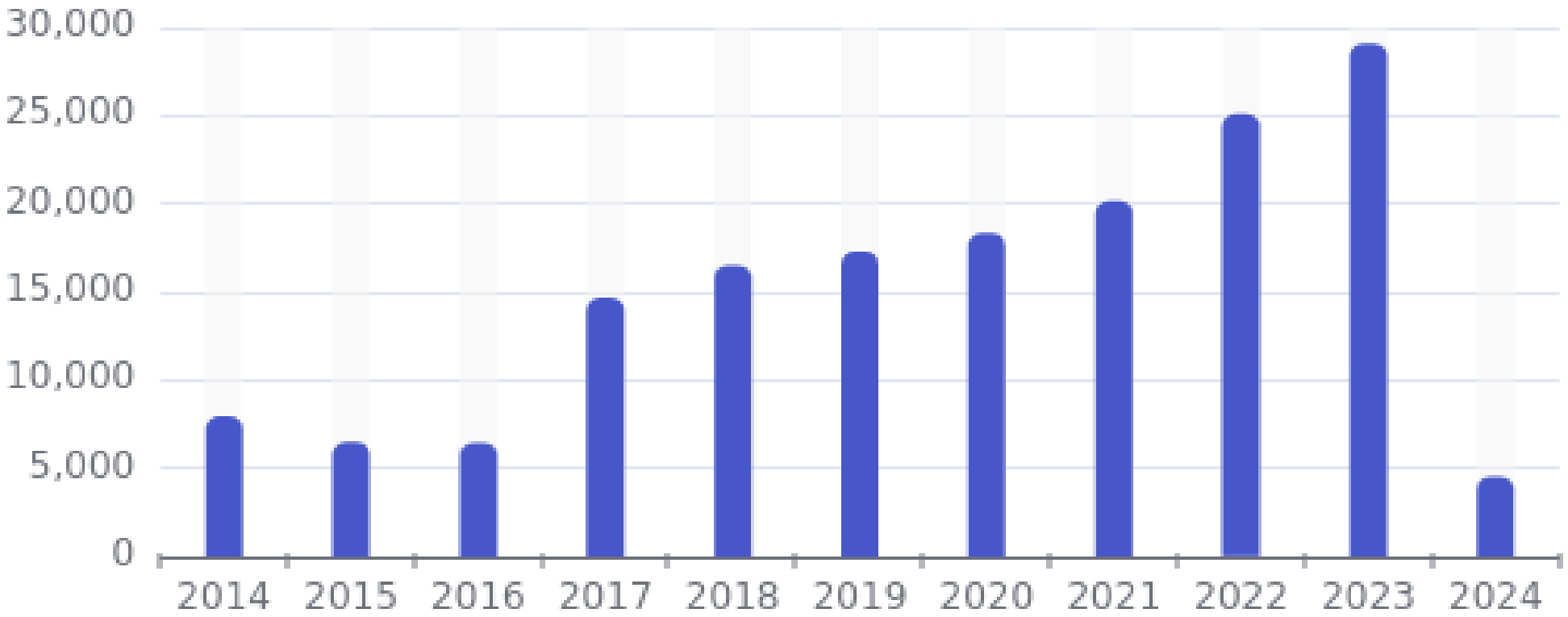
| | |
|---|---|
| CVSS Score | 9.3 |
| Confidentiality Impact | Complete (There is total information disclosure, resulting in all system files being revealed.) |
| Integrity Impact | Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.) |
| Availability Impact | Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code CSRF |
| CWE ID | 352 |

# CVSS

- CVSS = Common Vulnerability Scoring System
- Calcul du score
  - Doit être entre 0 et 10 → reflète la gravité de la vulnérabilité

    niveau faible / moyen / élevé ou critique
- Evaluation :
  - un score de base, qui permet d'évaluer un problème
    - impact théorique de la vulnérabilité
  - un score temporel, représentant les caractéristiques d'une vulnérabilité
    - pouvant évoluer en fonction d'exploits présents dans la nature, de correctifs…
  - un score environnemental, qui prend en compte l'environnement et les conséquences de l'exploitation de cette vulnérabilité.
    - Il évoluera en fonction des corrections existantes, des mesures palliatives, etc

# CVE : Les vulnérabilités (1/3)




https://www.cvedetails.com/browse-by-date.php

# CVE : Les vulnérabilités (2/3)

## Wordpress » Wordpress : Vulnerability Statistics

Vulnerabilities (338) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (0) Patches (20) Inventory Definitions (0) Compliance Definitions (0)

Vulnerability Feeds & Widgets

### Vulnerability Trends Over Time

| Year | # of Vulnerabilities | DoS | Code Execution | Overflow | Memory Corruption | Sql Injection | XSS | Directory Traversal | Http Response Splitting | Bypass something | Gain Information | Gain Privileges | CSRF | File Inclusion | # of exploits |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2004 | 2 | | | | | | 1 | | 1 | | | | | | |
| 2005 | 10 | | 5 | | | 3 | 2 | | | | 3 | | | | |
| 2006 | 16 | 1 | 2 | | | 1 | 5 | 1 | | | 3 | | | | |
| 2007 | 40 | 2 | 13 | | | 7 | 19 | | | 3 | 5 | | 2 | | 1 |
| 2008 | 28 | 2 | 5 | | | 3 | 9 | 4 | | 1 | 2 | | 2 | | |
| 2009 | 14 | 3 | 1 | | | | 3 | | | 1 | 3 | 1 | | | 4 |
| 2010 | 2 | | 1 | | | 1 | | | | | | | | | |
| 2011 | 11 | | | | | 1 | 2 | | | | 4 | | | | |
| 2012 | 21 | 2 | 1 | | | 1 | 7 | | | 5 | 3 | | 3 | | 6 |
| 2013 | 18 | 1 | 1 | | | | 7 | | | 3 | 2 | | 1 | | |
| 2014 | 28 | 3 | 3 | | | 1 | 8 | | | 6 | 2 | | 3 | 1 | |
| 2015 | 11 | 1 | 2 | | | 1 | 7 | | | 1 | 1 | | 1 | | |
| 2016 | 22 | 1 | 2 | | | | 9 | | | 6 | 1 | | 1 | | |
| 2017 | 46 | 1 | 1 | | | 4 | 17 | 4 | | 5 | 2 | | 5 | | |
| 2018 | 18 | 1 | 4 | | | | 5 | 1 | | 3 | 1 | | | | |
| 2019 | 23 | | 4 | | | | 12 | 1 | | 2 | 2 | | 2 | | |
| 2020 | 21 | 1 | 2 | | | | 7 | | | | | 2 | 1 | | |
| 2021 | 7 | | | | | | 2 | | | 2 | 2 | | | | |
| Total | 338 | 19 | 47 | | | 23 | 122 | 11 | 1 | 38 | 36 | 3 | 21 | 1 | 11 |
| % Of All | | 5.6 | 13.9 | 0.0 | 0.0 | 6.8 | 36.1 | 3.3 | 0.3 | 11.2 | 10.7 | 0.9 | 6.2 | 0.3 | |

# CVE : Les vulnérabilités (3/3)

## Vulnerability Details : CVE-2019-17669

WordPress before 5.2.4 has a Server Side Request Forgery (SSRF) vulnerability because URL validation does not consider the interpretation of a name as a series of hex characters.

Publish Date : 2019-10-17 Last Update Date : 2019-11-05

Collapse All Expand All Select Select&Copy ▼ Scroll To ▼ Comments ▼ External Links

Search Twitter Search YouTube Search Google

### - CVSS Scores & Vulnerability Types

| | |
|---|---|
| CVSS Score | 7.5 |
| Confidentiality Impact | Partial (There is considerable informational disclosure.) |
| Integrity Impact | Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.) |
| Availability Impact | Partial (There is reduced performance or interruptions in resource availability.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | |
| CWE ID | 918 |

### - Products Affected By CVE-2019-17669

| # | Product Type | Vendor | Product | Version | Update | Edition | Language | |
|---|---|---|---|---|---|---|---|---|
| 1 | Application | Wordpress | Wordpress | * | * | * | * | Version Details Vulnerabilities |

### - Number Of Affected Versions By Product

| Vendor | Product | Vulnerable Versions |
|---|---|---|
| Wordpress | Wordpress | 1 |

### - References For CVE-2019-17669

https://www.debian.org/security/2020/dsa-4599
DEBIAN DSA-4599

https://seclists.org/bugtraq/2020/Jan/8
BUGTRAQ 20200108 [SECURITY] [DSA 4599-1] wordpress security update

# Exemple représentation

| Editeur | Produit | Identifiant CVE | Score CVSS | Type de vulnérabilité | Date de publication | Exploitabilité (Preuve de concept publique) | Publications CERT-FR | Avis éditeur | Moyens de détection publiés par l'ANSSI | Moyens de détection (non qualifiés par l'ANSSI) |
|---|---|---|---|---|---|---|---|---|---|---|
| Microsoft | Exchange | CVE-2021-34473 | 9.8 | Exécution de code arbitraire à distance | 13/07/2021 | OUI | CERTFR-2021-ALE-017 | CVE-2021-34473 | Règle Sigma ANSSI : ProxyShell ProxyLogon | Règle Sigma : ProxyShell |
| Microsoft | Exchange | CVE-2021-34523 | 9.8 | Exécution de code arbitraire à distance | 13/07/2021 | OUI | CERTFR-2021-ALE-017 | CVE-2021-34523 | Règle Sigma ANSSI : ProxyShell ProxyLogon | Règle Sigma : ProxyShell |

https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

# Antivirus / Antimalware / Antispyware (1/3)


- Ces logiciels peuvent être :
  - Gratuits :
    - installé par défaut lors de l'achat du terminal ou par l'éditeur du système d'exploitation (Microsoft Security Essential) ;
    - ou manuellement : Comodo, Avast, Malwarebytes.
  - Payants : par exemple McAfee, Norton Antivirus.
- Ils nécessitent des mises à jour pour détecter les nouveaux codes malveillants :
  - du moteur
  - de la base antivirale
- Lors de l'apparition d'un nouveau code malveillant,
  - des éditeurs de solutions antivirales effectuent des analyses afin de :
    - déterminer la « signature » de ce code malveillant pour l'identifier de manière unique ;
    - identifier les moyens de protection et des corrections ;
    - enrichir leur base antivirale avec ces informations.

Éviter d'exécuter les scans gratuits depuis les pages Internet vous indiquant que votre ordinateur est infecté.

# Antivirus / Antimalware / Antispyware (2/3)

- Doivent être configurés de manière à :
  - Télécharger automatiquement les nouvelles signatures (base antivirale) ;
  - Être toujours actif (faire attention si votre antivirus est désactivé) ;
  - Scanner tout l'ordinateur sans exception de répertoires / fichiers ;
  - Effectuer des analyses complètes de manière périodique ;
  - Analyser automatiquement de nouveaux périphériques tel que les clés USB ;
  - Analyser les emails (entrants et sortants) et la messagerie instantanée.

# Antivirus / Antimalware / Antispyware (2/3)

- Limites
  - Il n’y a pas de base exhaustive pour les virus ;
  - Un code malveillant peut sévir dans un système disposant d’un antivirus et y demeuré indétecté ;
  - Les antivirus ne détectent que les virus dont les signatures sont « connues » ;
  - De très nombreux codes malveillants sont créés chaque jour.

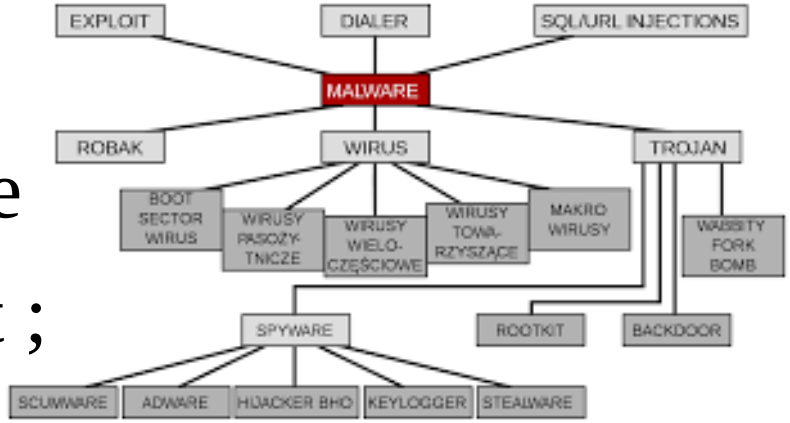
L’antivirus n’est pas une « arme absolue ».
La mise à jour des systèmes et des applications, ainsi qu’une bonne hygiène informatique sont indispensables.

# Code malveillants : Symptômes (1/2)

- Ralentissement
  - du terminal : exemple pendant l'arrêt et le redémarrage ;
  - du débit : la bande passante semble partagée.
- Ouvertures régulières de fenêtres de pop-up et de publicités ;
- Modification de la configuration de votre navigateur web
  - Modification de votre page d'accueil ou de votre moteur de recherche ;
    - Exemple : Snapdo.
  - Présence de nouvelles extensions que vous n'avez pas installées.
- Surconsommation des ressources
  - Réduction de l'espace libre sur disque sans raison ;
  - surcharge du processeur.

# Code malveillants : Symptômes (2/2)

- L’antivirus/anti-malware ou pare-feu
  - est désactivé sans votre intervention ;
- Les mises à jour
  - système/antivirus/anti-malware
    - → échouent systématiquement ;
- Messagerie
  - Vos contacts (amis/famille)
    - reçoivent des messages que vous n’avez pas envoyés ;
  - Votre boite d’envoi
    - contient des messages que vous n’avez pas envoyé.



# Protéger les données

- Lors des échanges par mail
  - chiffrer les pièces jointes ou les données sensibles
    - exemple : AxCrypt, Zed Container ;
    - envoyer le mot de passe (Clé) par un autre moyen : SMS.
- Lors de l'usage du Cloud
    - utiliser des logiciels spécialisés pour protéger/chiffrer vos données dans le Cloud (DropBox, Box, SkyDrive…).
- En effectuant des sauvegardes
  - Disque externe
  - Cloud

VIIVO EnCrypted Cloud alephcloud Safebox

Chiffrer vos données sensibles avant de les stocker.

# Durcissement de configuration des équipements (1/2)

- Modifier les mots de passe des comptes par défaut ;
  - exemple : administrateur.
- Désinstaller les logiciels/services inutiles (exemple : partage de fichiers) ;
- Désactiver les ports/lecteurs non utilisés ;
  - port série / port USB ;
  - lecteur de disquette ;
  - désactiver le « débogage USB » sur les téléphones.

# Durcissement de configuration des équipements (2/2)

- Mettre un mot de passe BIOS lors de la phase de démarrage
  - Lors du démarrage du poste, appuyer sur « F2 » pour rentrer dans le Setup
  - Aller dans l'onglet « Security » pour saisir les mots de passe.
- Désactiver le boot sur des périphériques externes (clé USB, CD Rom)
  - Dans le setup (Touche « F2 » lors du démarrage), configurer l'ordre de démarrage pour avoir le disque dur en premier.
  - Activer la journalisation.

# A retenir

- La sécurité applicative ne doit pas être négliger
- La TMA est une brique importante


https://school.hello-design.fr

3H

# La suite de la Session 3 ???

- La suite de cette partie
  - Rendez vous la semaine prochaine

# Rendez-vous au prochain cours

- Merci de votre attention