SÉCURITÉ DES APPLICATIONS

POEC Consultant - 2024

OBJECTIF DU MODULE

Connaître les bonnes pratiques de sécurité et les failles communément exploitées dans le domaine applicatif.

Connaître ses obligations face au Règlement Général de Protection des Données.

GÉNÉRALITÉS

GÉNÉRALITÉS – RAPPELS

Définition des termes :

- **Cybersécurité** vs **cyberdéfense**
- **SSI**, **pentest**…

Dans un contexte professionnel :

- ne dites plus **cybersécurité**, mais **SSI**
- ne dites plus **hacking** mais **pentest** !

Sécurité des systèmes d'informations :

- Ensemble de ressources, à la fois **humaines**, **matérielles** et **immatérielles** dont le rôle est de **collecter**, **stocker**, **traiter** et **distribuer** de l'information.

GÉNÉRALITÉS – PISTES DE RÉFLEXION

Pourquoi y a-t-il souvent des failles de sécurité dans les applications ?

Quelles sont les informations sensibles pour une entreprises ?

Que connaissez-vous comme bonne pratique de sécurité ?

Un exemple de système 100% inviolable ?

GÉNÉRALITÉS – LE CAHIER DES CHARGES

- Protéger le patrimoine opérationnel de l'entreprise (les bases de données, les documents, les accès divers),
- Répondre aux obligations et responsabilités légales des dirigeants dans l'exploitation et la maîtrise de leur système d'information
  - L'élaboration de règles et de procédures
  - La définition des actions à entreprendre et des personnes responsables
  - La détermination du périmètre concerné

GÉNÉRALITÉS – LA MISE EN ŒUVRE

- La confidentialité
- L'intégrité
- La disponibilité
- La traçabilité des données

GÉNÉRALITÉS – LA SÉCURITÉ EN ENTREPRISE

Au niveau utilisateurs :

- Comprendre l'importance de leur position

Au niveau des technologies :

- Droits d'accès des utilisateurs

Au niveau physique :

- L'accès à l'infrastructure, au matériel …

+

- Mettre en place une charte informatique.
- Réaliser des guides Utilisateurs.
- Filtrer les accès aux données.

−

- Ne pas laisser les identifiants par défaut.
- Ne pas stocker les identifiants sur un post-it.
- Verrouiller sa session de poste.

GÉNÉRALITÉS – LES BONNES PRATIQUES (ANSSI)

1. Choisir avec soin ses mots de passe
2. Mettre à jour régulièrement vos logiciels
3. Bien connaître ses utilisateurs et ses prestataires
4. Effectuer des sauvegardes régulières
5. Sécuriser l'accès Wi-Fi de votre entreprise
6. Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur
7. Protéger ses données lors de ses déplacements
8. Être prudent lors de l'utilisation de sa messagerie
9. Télécharger les programmes sur les sites officiels des éditeurs
10. Être vigilant lors d'un paiement sur Internet
11. Séparer les usages personnels des usages professionnels
12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Source : https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

KASPERSKY lab

LES 12 BONNES PRATIQUES

Sécurité informatique

METTRE À JOUR
le système d'exploitation
et les logiciels

Choisir des
MOTS DE PASSE COMPLEXES
combinant majuscules,
minuscules,chiffres

Se méfier des clés USB
et des disques durs
EXTERNES

Effectuer des
SAUVEGARDES
régulières

VERROUILLER VOTRE SESSION
dès que vous vous absentez

Installer, utiliser
et mettre à jour
une suite de
SÉCURITÉ ANTIVIRUS

Utiliser
un logiciel de
GESTION DE MOT DE PASSE
et désactiver celui
des navigateurs

Ne jamais saisir vos
DONNÉES PERSONNELLES
sur des sites qui n'offrent pas
toutes les garanties requises

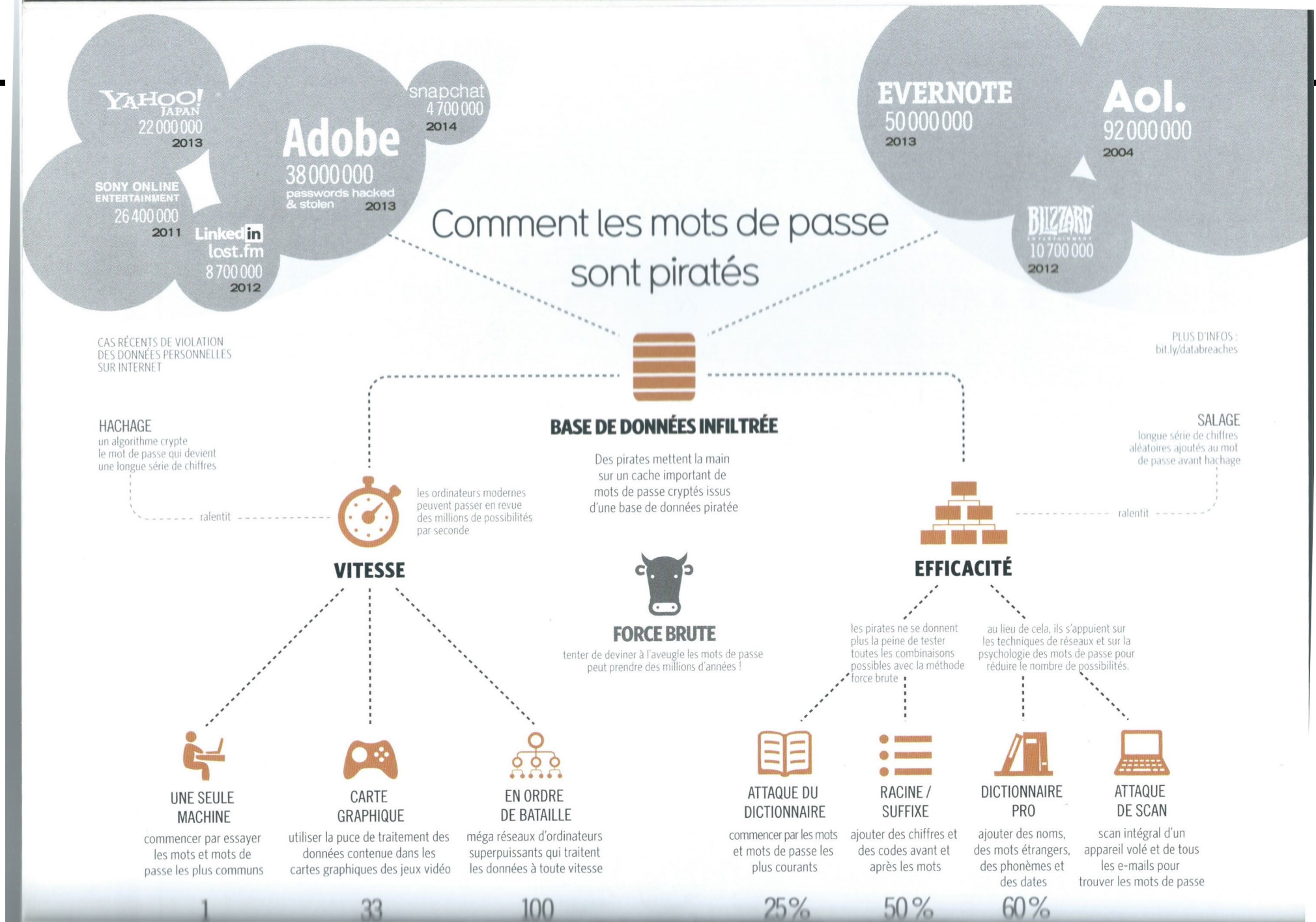
NE JAMAIS CLIQUER SUR UN LIEN
dans un email vous demandant
de vous identifier

Ne jamais ouvrir
les pièces jointes avec les
EXTENSIONS :
.pif, .bat, .com, .exe, .lnk...

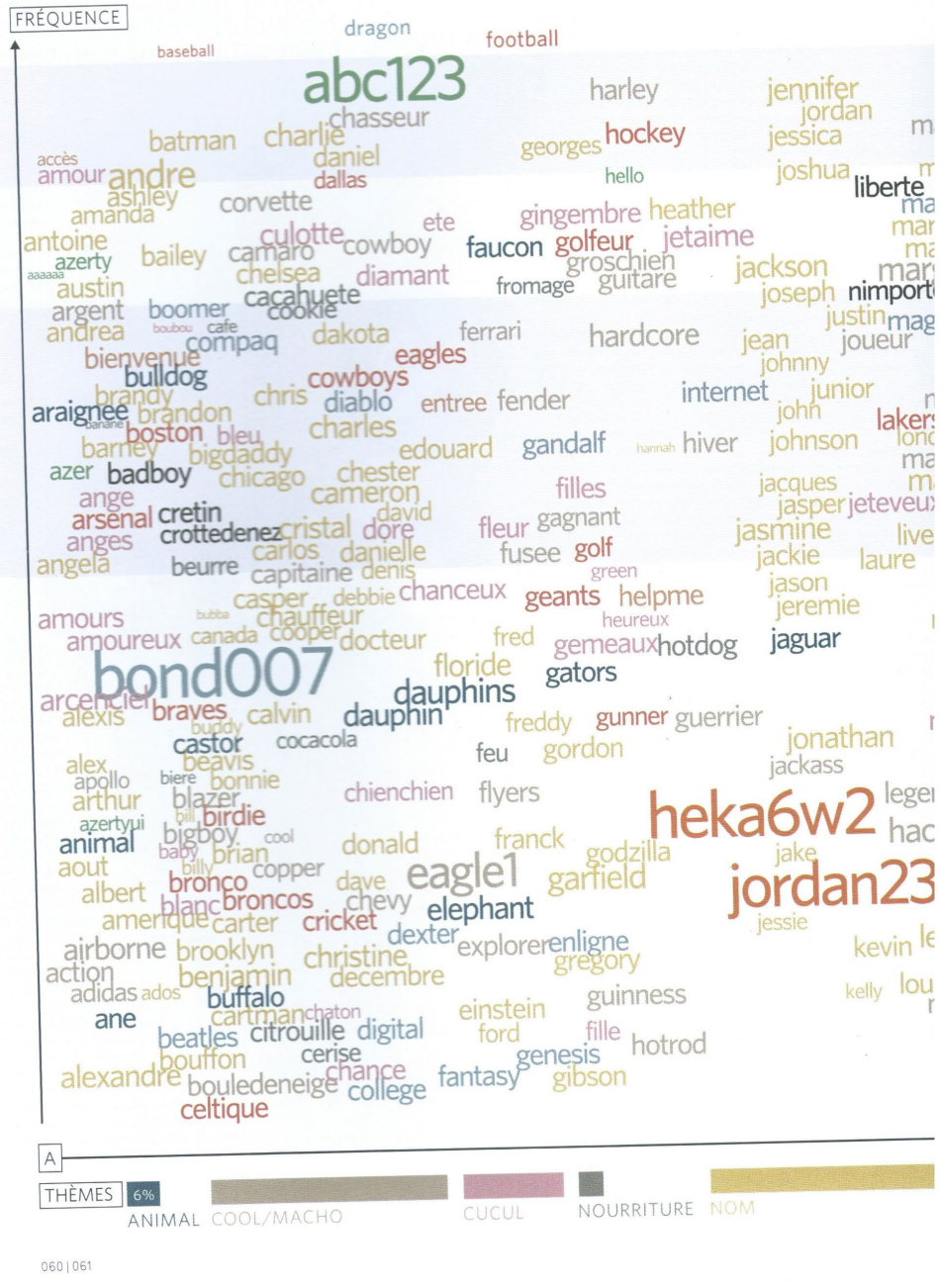
CHANGER RÉGULIÈREMENT
de mot de passe

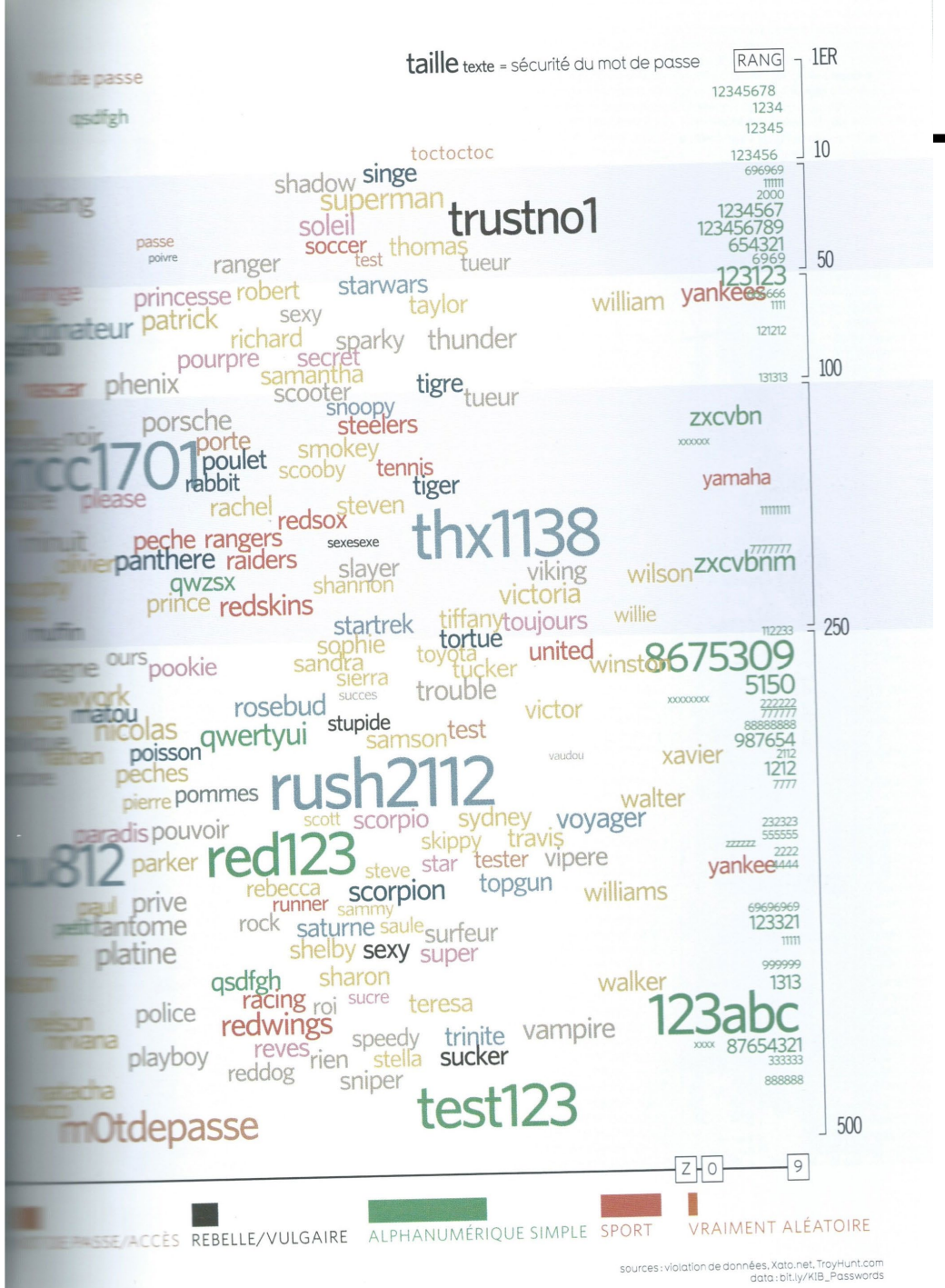
CHIFFRER
les données sensibles
sur votre PC

www.kaspersky.fr

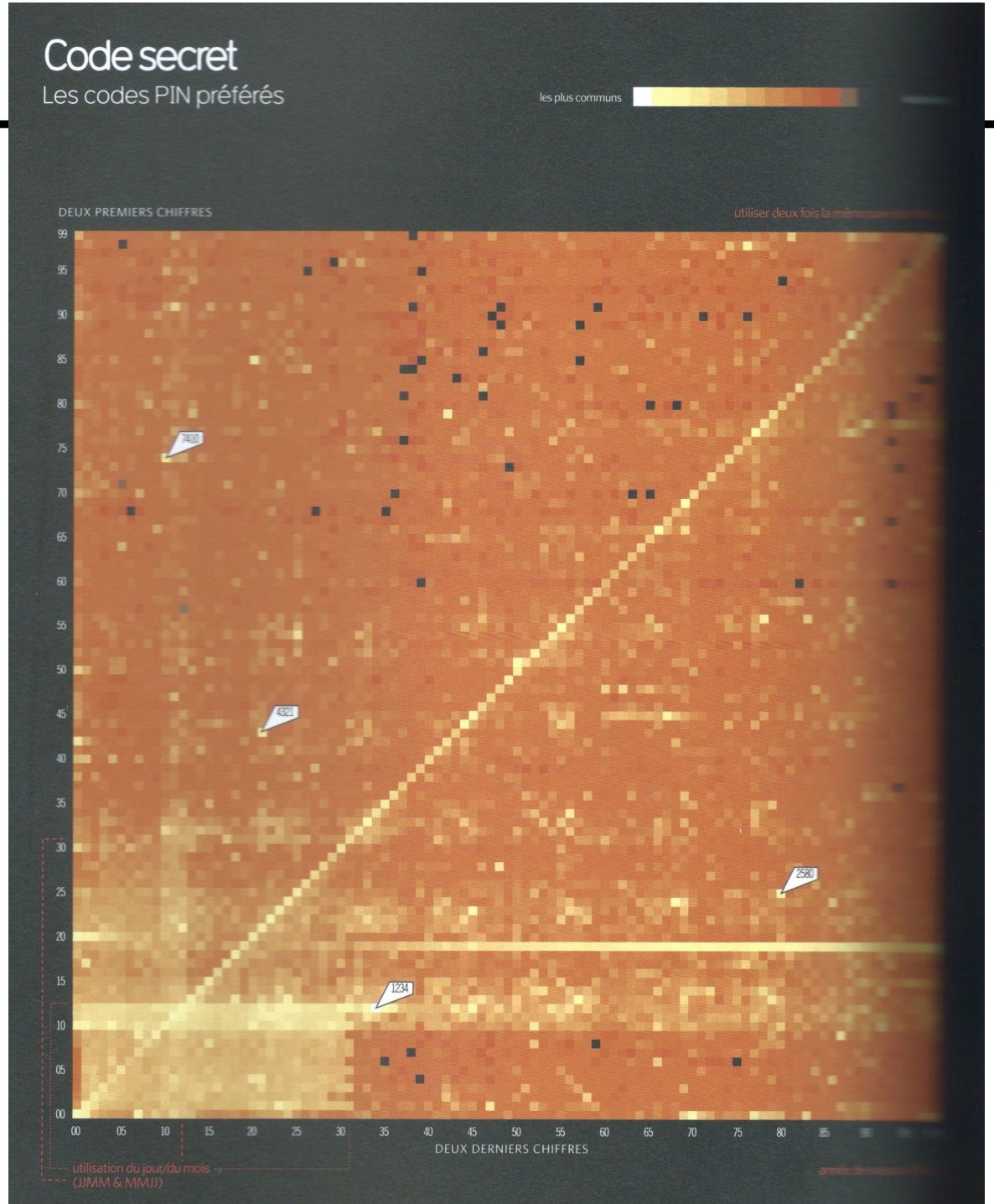

YAHOO! JAPAN
22 000 000
2013
SONY ONLINE ENTERTAINMENT
26 400 000
2011
Linkedin
last.fm
8 700 000
2012
Adobe
38 000 000
passwords hacked & stolen
2013
snapchat
4 700 000
2014
EVERNOTE
50 000 000
2013
Aol.
92 000 000
2004
BLIZZARD ENTERTAINMENT
10 700 000
2012
Comment les mots de passe sont piratés
CAS RÉCENTS DE VIOLATION DES DONNÉES PERSONNELLES SUR INTERNET
PLUS D'INFOS : bit.ly/databreaches
BASE DE DONNÉES INFILTRÉE
Des pirates mettent la main sur un cache important de mots de passe cryptés issus d'une base de données piratée
HACHAGE
un algorithme crypte le mot de passe qui devient une longue série de chiffres
ralentit
les ordinateurs modernes peuvent passer en revue des millions de possibilités par seconde
SALAGE
longue série de chiffres aléatoires ajoutés au mot de passe avant hachage
ralentit
VITESSE
EFFICACITÉ
FORCE BRUTE
tenter de deviner à l'aveugle les mots de passe peut prendre des millions d'années !
les pirates ne se donnent plus la peine de tester toutes les combinaisons possibles avec la méthode force brute
au lieu de cela, ils s'appuient sur les techniques de réseaux et sur la psychologie des mots de passe pour réduire le nombre de possibilités.
UNE SEULE MACHINE
commencer par essayer les mots et mots de passe les plus communs
1
CARTE GRAPHIQUE
utiliser la puce de traitement des données contenue dans les cartes graphiques des jeux vidéo
33
EN ORDRE DE BATAILLE
méga réseaux d'ordinateurs superpuissants qui traitent les données à toute vitesse
100
ATTAQUE DU DICTIONNAIRE
commencer par les mots et mots de passe les plus courants
25%
RACINE / SUFFIXE
ajouter des chiffres et des codes avant et après les mots
50 %
DICTIONNAIRE PRO
ajouter des noms, des mots étrangers, des phonèmes et des dates
60 %
ATTAQUE DE SCAN
scan intégral d'un appareil volé et de tous les e-mails pour trouver les mots de passe

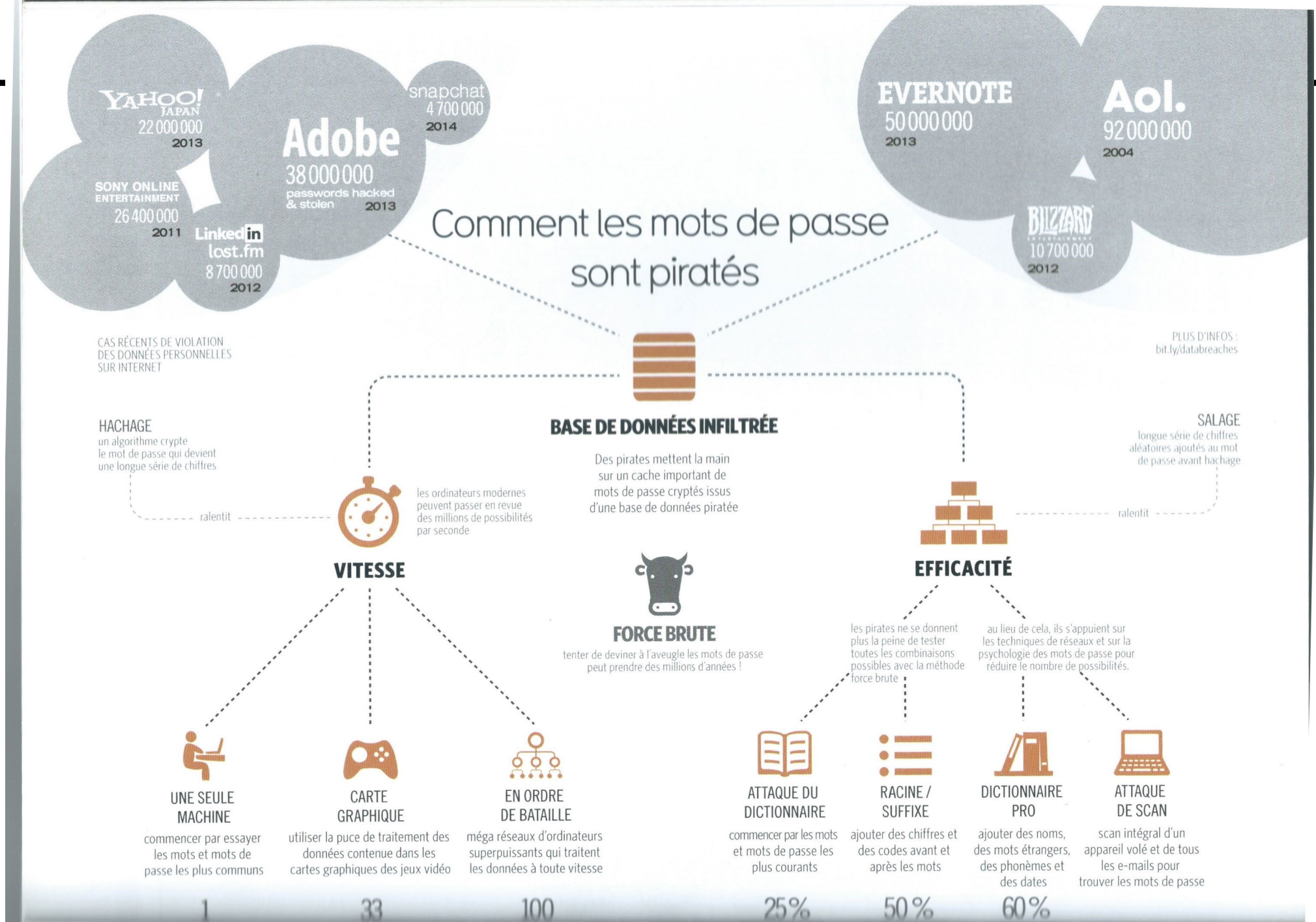
Les 500 mots de passe les plus courants Le vôtre en fait-il





sources : violation de données, Xato.net, TroyHunt.com
data : bit.ly/KIB_Passwords


Code secret
Les codes PIN préférés
les plus communs
DEUX PREMIERS CHIFFRES
utiliser deux fois la même
7431
4321
2580
1234
99
95
90
85
80
75
70
65
60
55
50
45
40
35
30
25
20
15
10
05
00
00 05 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85
DEUX DERNIERS CHIFFRES
utilisation du jour/du mois
(JJMM & MMJJ)


YAHOO! JAPAN
22 000 000
2013
SONY ONLINE ENTERTAINMENT
26 400 000
2011
Linkedin
last.fm
8 700 000
2012
Adobe
38 000 000
passwords hacked & stolen
2013
snapchat
4 700 000
2014
EVERNOTE
50 000 000
2013
Aol.
92 000 000
2004
BLIZZARD ENTERTAINMENT
10 700 000
2012
Comment les mots de passe sont piratés
CAS RÉCENTS DE VIOLATION DES DONNÉES PERSONNELLES SUR INTERNET
PLUS D'INFOS : bit.ly/databreaches
BASE DE DONNÉES INFILTRÉE
Des pirates mettent la main sur un cache important de mots de passe cryptés issus d'une base de données piratée
HACHAGE
un algorithme crypte le mot de passe qui devient une longue série de chiffres
ralentit
les ordinateurs modernes peuvent passer en revue des millions de possibilités par seconde
SALAGE
longue série de chiffres aléatoires ajoutés au mot de passe avant hachage
ralentit
VITESSE
EFFICACITÉ
FORCE BRUTE
tenter de deviner à l'aveugle les mots de passe peut prendre des millions d'années !
les pirates ne se donnent plus la peine de tester toutes les combinaisons possibles avec la méthode force brute
au lieu de cela, ils s'appuient sur les techniques de réseaux et sur la psychologie des mots de passe pour réduire le nombre de possibilités.
UNE SEULE MACHINE
commencer par essayer les mots et mots de passe les plus communs
1
CARTE GRAPHIQUE
utiliser la puce de traitement des données contenue dans les cartes graphiques des jeux vidéo
33
EN ORDRE DE BATAILLE
méga réseaux d'ordinateurs superpuissants qui traitent les données à toute vitesse
100
ATTAQUE DU DICTIONNAIRE
commencer par les mots et mots de passe les plus courants
25%
RACINE / SUFFIXE
ajouter des chiffres et des codes avant et après les mots
50 %
DICTIONNAIRE PRO
ajouter des noms, des mots étrangers, des phonèmes et des dates
60 %
ATTAQUE DE SCAN
scan intégral d'un appareil volé et de tous les e-mails pour trouver les mots de passe

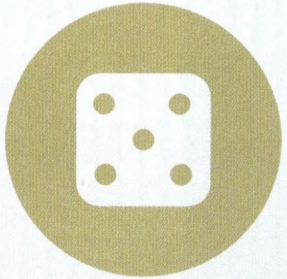
GÉNÉRALITÉS – DÉLAI DE PIRATAGE DES MOTS DE PASSE

Nombre de caractères	Uniquement des chiffres	Lettres minuscules	Lettres minuscules et majuscules	Lettres minuscules et majuscules + chiffres	Lettres min. et maj. + chiffres + caractères spéciaux
4	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT
6	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	1 sec	5 sec
8	IMMÉDIAT	5 sec	22 min	1 heure	8 heures
10	IMMÉDIAT	58 min	1 mois	7 mois	5 ans
12	25 sec	3 semaines	300 ans	2 000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d'années	200 millions d'années
16	2 jours	34 000 ans	2 milliards d'années	37 milliards d'années	1 milliard de milliards d'années

Source 2020

moins de
3 heures

Comment créer un mot de passe qui résiste au piratage



ALPHANUMÉRIQUE ALÉATOIRE

créé par un générateur de mots de passe et administré par un gestionnaire de mots de passe

ex. : $9Eh7*8I1m0p&

« Quand j'avais sept ans, ma sœur a jeté ma peluche dans les toilettes... »

« Waouh... ce canapé sent vraiment mauvais »

« Il était une fois dans une galaxie très très éloignée »

Qja7amsajmpdlt...

Waouh...ccsvm

Ie1-fois@1-gtte

TRANSFORMER UNE PHRASE MÉMORISABLE EN MOT DE PASSE

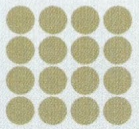
choisissez une phrase dont vous allez vous souvenir et faites-en un mot de passe

lancé par le chercheur en sécurité Bruce Schneier

Conseils

NE RÉUTILISEZ JAMAIS UN BON MOT DE PASSE

utilisez des mots de passe uniques pour les services les plus importants et les données les plus sensibles



AU MOINS 12 CARACTÈRES

différence entre le temps nécessaire pour craquer un mot de passe alphanumérique de 12 caractères *versus* un mot de passe de 8 caractères ? 200 ans

DOUBLE AUTHENTIFICATION

Google et beaucoup d'autres sites vous permettent d'utiliser votre mobile pour entrer un deuxième mot de passe

sources : BoingBoing.net, Arstechnica
data : bit.ly/KIB_Passwords

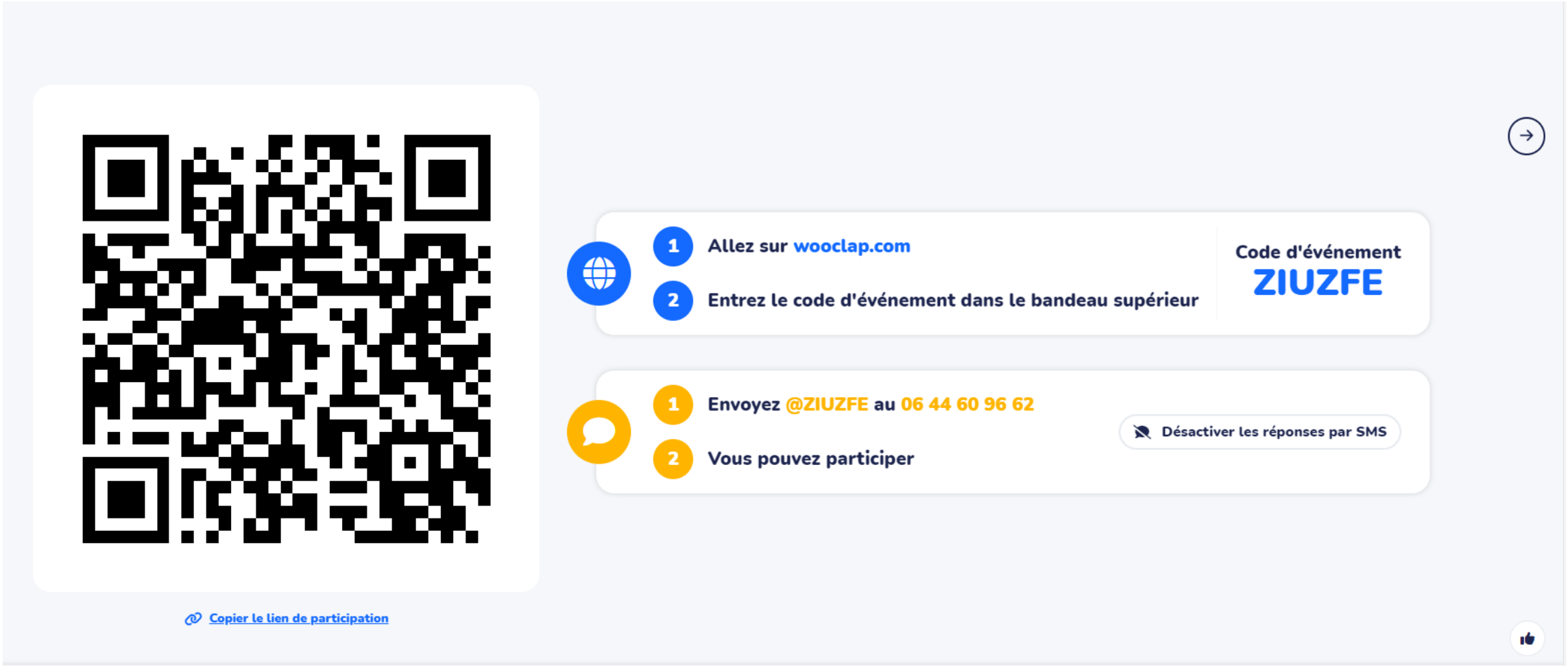
GÉNÉRALITÉS – QUELQUES BONNES PRATIQUES PERSO

- Tenir ses applications à jour : prendre au sérieux les alertes de sécurité dans le terminal (dépendances npm) ou reçue par mail
- Connaitre les failles communes, pour s'en protéger (chapitre 4)
- Appliquer un niveau raisonnable de sécurité, cf principe de Pareto (80 20)

GÉNÉRALITÉS – BYOD (BRING YOUR OWN DEVICE)

- Respecter la vie privée des collaborateurs.
- Vérifier les mises à jour de sécurité des équipements.
- Formaliser les responsabilités et préciser les précautions dans une charte.
- Soumettre l'utilisation des équipements personnels à l’autorisation d’un manager.

GÉNÉRALITÉS – WOOCLAP



GÉNÉRALITÉS – EXERCICE

Réaliser un plan de sensibilisation aux bonnes pratiques à destination des utilisateurs se trouvant à l'EPSI.

Groupe de 4 max et minimum 2.

RGPD

Le **R**èglement **G**énéral sur la **P**rotection des **D**onnées

RGPD – INTRODUCTION

Marie-Laure Denis
Présidente de la CNIL

- Naît d'un concours de circonstance gouvernemental.
- Dépend de la Loi Informatique et Libertés de 1978.
- Promeut le respect des citoyens, de leurs libertés.

La loi Informatique et Libertés a été révisée en 2004, les changements ont notamment donné naissance au CIL « Correspondant Informatique et Libertés ».

Source : La loi de 2004 et l'introduction du CIL

RGPD – LES OBJECTIFS

Garantir la protection de la vie privée et des libertés

3 Axes majeurs du RGPD

1. Renforcer les pouvoirs de sanction des autorités
2. Responsabiliser les acteurs de traitements des données
3. Renforcer les droits des personnes

RGPD – LES ACTEURS INSTITUTIONNELS

CNIL.

Autorité Administrative Indépendante en charge de réguler l'utilisation des données personnelles

Ses **4** missions

- Informer & protéger les droits
- Accompagner & Conseiller la conformité
- Anticiper & Innover
- Contrôler & Sanctionner

RGPD – LES ACTEURS INSTITUTIONNELS

Coordonner l'action des autorités nationales & conseiller les Etats membres de l'Union Européenne

Ses **4** missions

- Publier des directives relatives au RGPD
- Conseiller la Commission Européenne et les membres
- Se prononcer sur les litiges & Garantir l'uniformité
- Donner son avis sur les projets de décisions des AAI

RGPD – LES ACTEURS INSTITUTIONNELS

Veiller à l'application uniforme de la législation & sanctionner toute entité Publique ou Privée

COUR DE JUSTICE
DE L'UNION EUROPÉENNE

Cour de Justice

- Traiter les demandes d'interprétation de la législation
- Prendre & Réviser des décisions de justice
- Les décisions sont contraignantes juridiquement

Tribunal

- Statuer sur les recours en annulation

RGPD – LES DONNÉES À CARACTÈRE PERSONNEL

- Une note sur un post-it
- Un document papier
- Un fichier informatique
- Une photographie
- Un fichier vidéo
- Un enregistrement audio
- etc.

RGPD – LES DONNÉES À CARACTÈRE PERSONNEL

1. Des données **directement** identifiantes
2. Des données **indirectement** identifiantes
3. Toute **combinaison** d'informations permettant d'identifier la personne

RGPD – DES DONNÉES **DIRECTEMENT** IDENTIFIANTES

Un élément de donnée indique clairement l'identité de la personne

Données type : nom, prénom, email, photo, etc.

Où trouver ces données ?

- Les fichiers de paie
- Les relevés de compte
- Les devis
- Les factures
- Les fichiers clients
- etc.

RGPD – DES DONNÉES **INDIRECTEMENT** IDENTIFIANTES

L'association d'une donnée avec un élément d'une autre base de données permet de retrouver l'identité de la personne

Données type : n° client, n° de téléphone, etc.

Où trouver ces données ?

- Pseudo sur un réseau social
- Données biométriques
- Numéro de sécurité sociale (NIR)

RGPD – TOUTES LES **COMBINAISONS** D'INFORMATIONS

L'association de plusieurs données formant un caractère unique permettant de remonter à l'identité de la personne

Données type : n° client, n° de téléphone, etc.

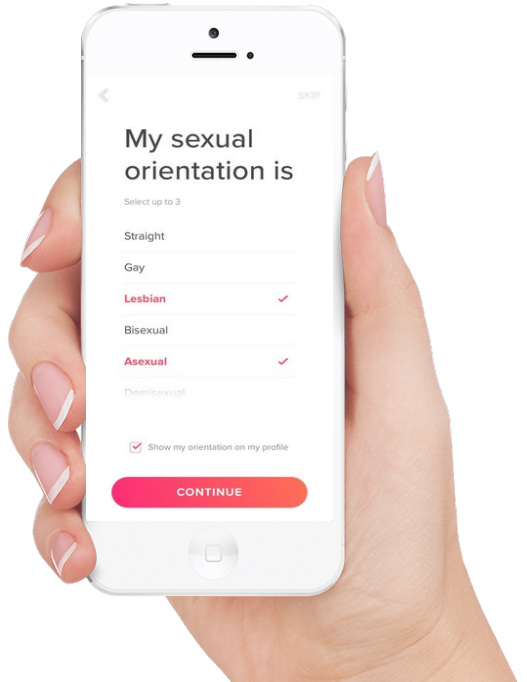
Où trouver ces données ?

- Loisirs & activités
- Date & Lieu de naissance
- Nom de l'employeur
- Lieu de résidence
- etc.

RGPD – LES DONNÉES DITES **SENSIBLES**

Ce sont des informations qui révèlent la prétendue orientation sexuelle, origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale.

- Le traitement des données sensibles est autorisé dans certains cas.
- Pour avoir lieu, l'individu doit donner son consentement écrit.
- Répond à des principes de licéité, loyauté, transparence.
- Exception faite, si le traitement est d'intérêt vital.



RGPD – LES ORGANISMES CONCERNÉS PAR L'APPLICATION DU RGPD

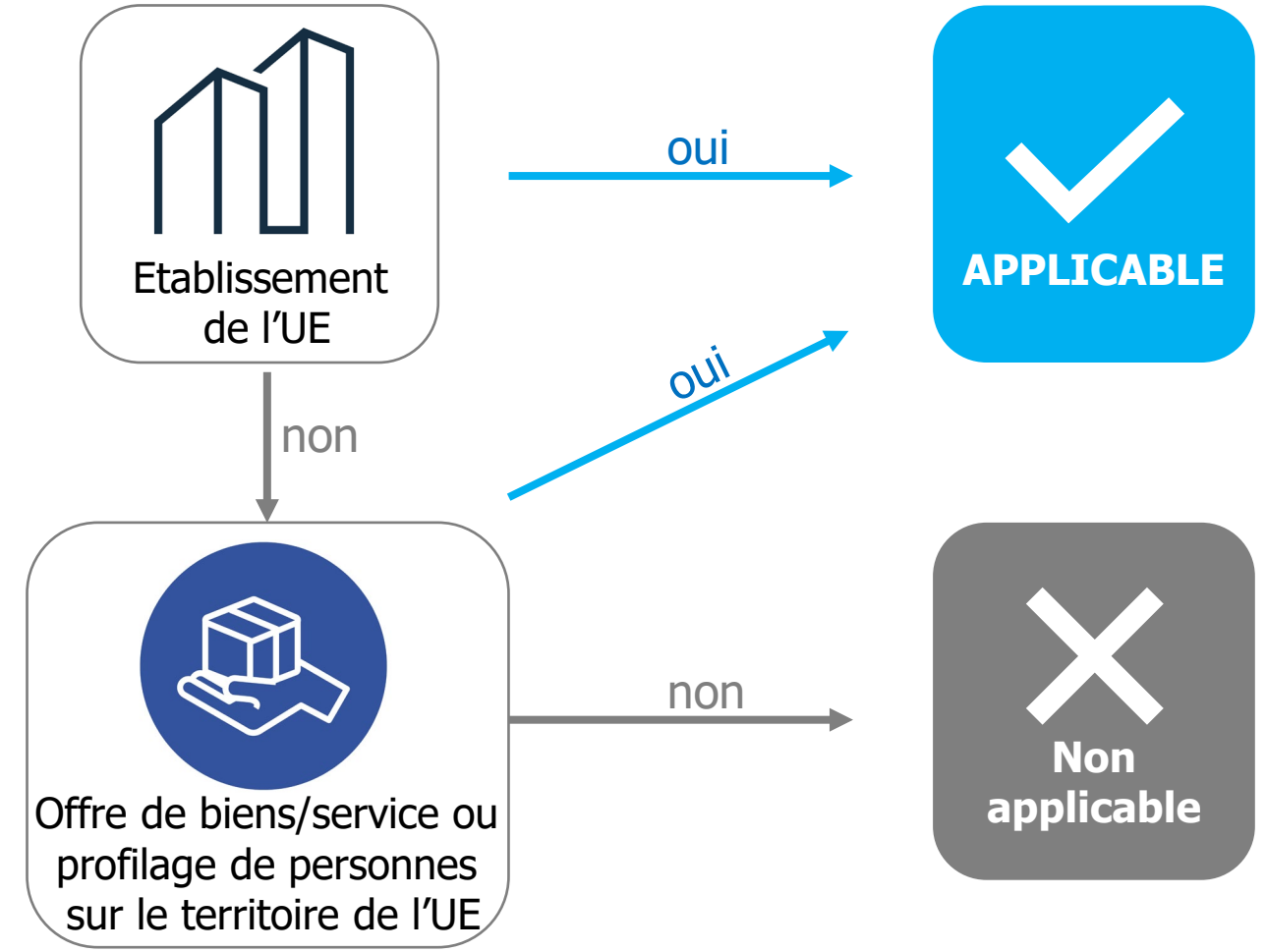
TOUS LES ORGANISMES PUBLICS & PRIVES

- Les entreprises (TPE, PME, ETI et GE)
- Les administrations
- Les collectivités
- Les associations

RGPD – LES ORGANISMES CONCERNÉS PAR L'APPLICATION DU RGPD

Critère de l'établissement

Critère de ciblage



RGPD – RESPONSABLE DE TRAITEMENT ET SOUS-TRAITANT

Un traitement de données peut être mis en œuvre par un organisme pour son propre compte, soit pour le compte et sur instruction d'un autre organisme

- **Responsable de Traitement (RT)**

  FINALITE = Déterminer le « pourquoi » / objectifs

  MOYENS = Déterminer le « comment »

OU

- **Sous-Traitant (ST)**

  Traiter les données pour le compte du RT

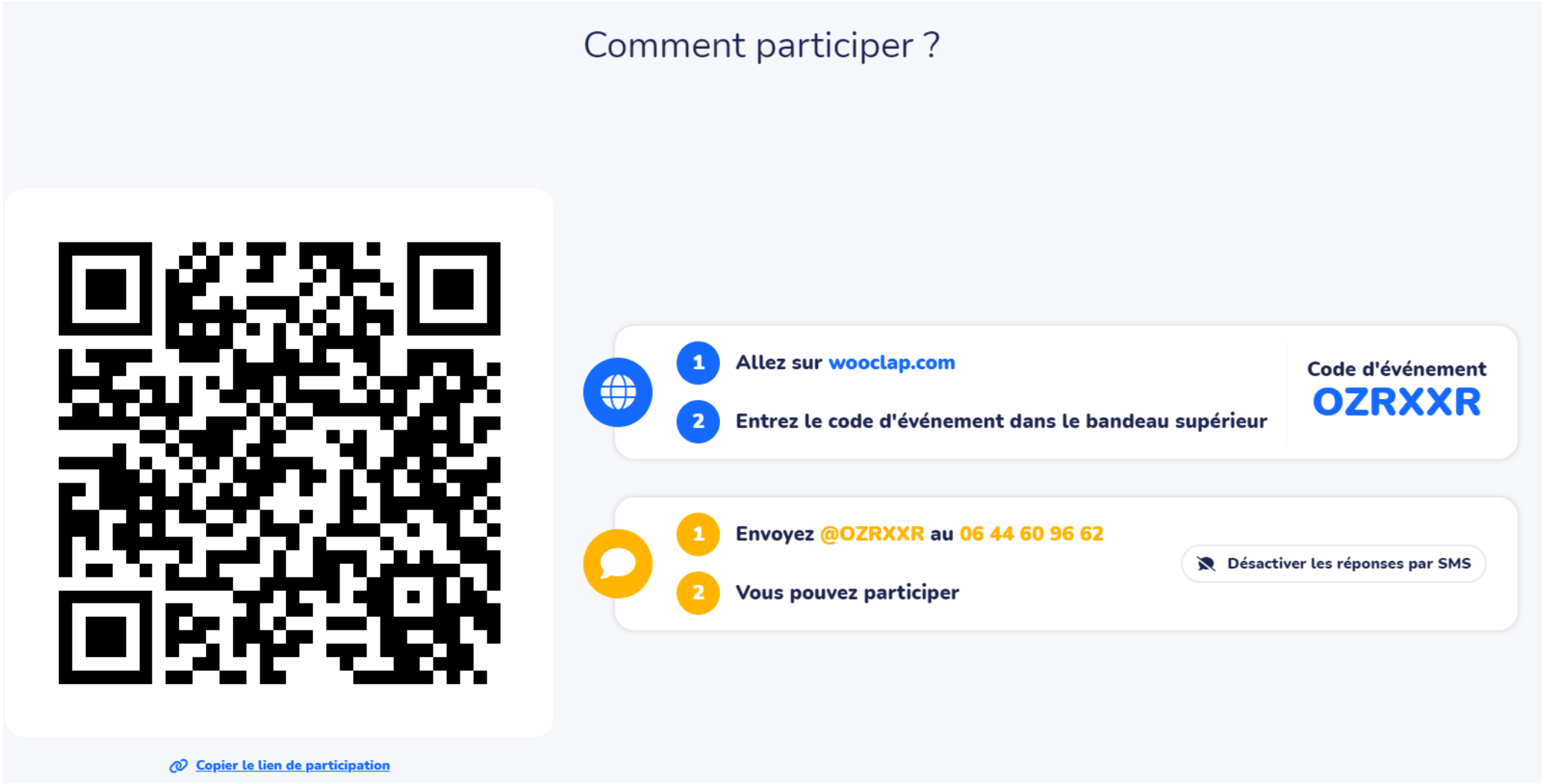
  Respecter les instructions du RT

RGPD – LES CONTRAINTES AU DÉVELOPPEMENT

- https://www.linkedin.com/posts/emmanuelmacron_les-etats-unis-ont-les-gafa-google-apple-activity-6742509736903614464-oc_A/

  Les Etats-Unis ont les GAFA (Google, Apple, Facebook et Amazon), la Chine a les BATX (Baidu, Alibaba, Tencent et Xiaomi). Et l'Europe ? Nous avons le RGPD. Il est temps d'avoir notre propre souveraineté technologique et de ne pas dépendre uniquement des solutions américaines ou chinoises !

RGPD – WOOCLAP



Principes de Protection des Données

PRINCIPES DE PROTECTION DES DONNÉES – LES 8 RÈGLES D'OR

- Finalité du traitement
- Licéité du traitement
- Minimisation des données
- Protection particulière des données sensibles
- Conservation limitée des données
- Obligation de sécurité
- Transparence
- Droits des personnes

RGPD – LA FINALITÉ DE TRAITEMENT

Objectif en vue duquel les données sont collectées, enregistrées, exploitées, transmises, conservées, etc. pour l'organisme.

Exemple de finalité

- La gestion des recrutements
- La gestion de la clientèle
- La gestion des usagers d'un service public
- etc.

La finalité est obligatoire, préalable au traitement, légal et légitime par rapport au contexte d'activité de l'organisme.

RGPD – LA FINALITÉ DE TRAITEMENT

Les finalités de traitement suivantes sont-elles explicites ?

- Recueillir les données des élèves
- Organiser la répartition des élèves par section
- Analyser la navigation des conducteurs automobiles
- Faire de la publicité ciblée
- Vidéo protection d'un salarié en continu
- Livraison à l'adresse du domicile d'un client
- Calcul d'une taxe au regard de la situation économique d'un client
- Géolocalisation des utilisateurs d'une application mobile de discussion

RGPD – LA FINALITÉ DE TRAITEMENT - EXEMPLES

Exemples de détournement

Fichiers des employés d'une société pour la gestion des ressources humaines et la masse salariale

- **Détournement** : transmission des adresses de messageries à une entreprise partenaire pour la prospection commerciale des salariés

Dispositif de géolocalisation des véhicules du personnel pour assurer la gestion des livraisons client.

- **Détournement** : utilisation du dispositif par ledit employeur afin de contrôler le temps de travail des salariés

RGPD – LA LICÉITÉ DU TRAITEMENT

Le traitement doit être explicitement permis ou ne pas être interdit.

- La personne concernée par le traitement a **donné son consentement** au traitement pour une ou des finalités explicites.
- Le traitement est **nécessaire à l'exécution d'un contrat** par lequel la personne concernée est partie prenante ou à l'origine de la demande du contrat
- Le traitement est **nécessaire au respect d'une obligation légale** pour le responsable de traitement
- Le traitement est **nécessaire à la sauvegarde des intérêts vitaux** de la personne concernée ou d'autre personne physique
- Le traitement est **nécessaire à l'exécution d'une mission** d'intérêt public ou relevant de l'exercice de l'autorité publique
- Le traitement est **nécessaire aux fins des intérêts légitimes** du responsable de traitement dans le respect de la législation et des droits de la personne concernée

RGPD – LA LICÉITÉ DU TRAITEMENT – LE CONSENTEMENT

Doit correspondre à un seul traitement et pour une finalité déterminée
Plusieurs finalités nécessitent plusieurs consentements pour chacune

Une information préalable est nécessaire, une information claire et compréhensible

- L'identité du RT
- Les finalités du traitement
- Les catégories de données collectées
- L'existence du droit de retrait

UNIVOQUE

Être donné sans ambiguïté par un acte positif

LIBRE

Ne doit être ni contraint ni influencé, un choix réel doit être offert à la personne

RGPD – LA LICÉITÉ DU TRAITEMENT – LA NÉCESSITÉ CONTRACTUELLE

- Exécution d'un contrat auquel par la personne concernée est partie prenante

- Exécution de mesures précontractuelles prises à la demande de la personne concernée

RGPD – LA LICÉITÉ DU TRAITEMENT – OBLIGATION LÉGALE

RESPECT D'OBLIGATION IMPOSÉE AU RT PAR LA LÉGISLATION OU LA RÉGLEMENTATION

Exemples

- Obligation de transmission d'information aux autorités publiques pour les institutions financières
- Obligation de l'employeur de mettre en œuvre des traitements pour la gestion fiscale et sociale

RGPD – LA LICÉITÉ DU TRAITEMENT – SAUVEGARDE DES INTÉRÊTS VITAUX

UTILISÉ UNIQUEMENT LORSQU'IL EST IMPOSSIBLE DE RECOURIR À UN AUTRE FONDEMENT

Exemples

- Menace de la vie de la personne
- Incapacité physique d'exprimé le consentement
- Gestion de certaines problématiques humanitaires (Catastrophes, épidémies, rapatriements, etc.)

RGPD – LA LICÉITÉ DU TRAITEMENT – L'INTÉRÊT PUBLIC

EXÉCUTION D'UNE MISSION D'INTÉRÊT PUBLIC OU RELEVANT DE L'EXERCICE DE L'AUTORITÉ PUBLIQUE

Limitation

Le Responsable de Traitement doit être compétent sur la mission d'intérêt publique qui relève de la finalité poursuivie

Exemples

- Gestion des inscriptions scolaires
- Délivrances de subventions par le Conseil Départementale à des associations

RGPD – LA LICÉITÉ DU TRAITEMENT – INTÉRÊTS LÉGITIMES

MISE EN BALANCE DES INTÉRÊTS POUR LE RT ET LES DROITS DE LA PERSONNE CONCERNÉE

La personne peut-elle raisonnablement s'attendre à ce que des données à caractère personnel soient objet d'un traitement pour cette finalité ?

Exemples

- Utilisation de vidéosurveillance aux fins de protéger les biens et personnes au sein d'un établissement
- Communication d'une association à ses membres sur son actualité

RGPD – BONNES PRATIQUES

Une donnée est pertinente si elle a un lien direct avec la finalité du traitement.

Des données inexactes peuvent porter préjudice aux personnes concernées.

1. Vérifier la nature, la quantité et la précision des données collectées
2. Existe-t-il une autre solution moins intrusive pour la personne ?
3. **JAMAIS** collecter à titre préventif ! ! !
4. Anonymiser les données dès la conservation, garder l'identification n'est pas nécessaire
5. Limiter les zones de commentaires libres et privilégier les choix multiples

RGPD – CONSERVATION DES DONNÉES

Préserver le « droit à l'oubli » ?

- Effacer les données
- Anonymiser les données afin de rendre impossible l'identification
- Archiver les données sous certaines conditions

Qui décide des actions et du temps ?

Le Responsable de Traitement

RGPD – CONSERVATION DES DONNÉES - EXEMPLES

Bulletin de paie

- Conserver 5 ans après la remise au salarié

Dossier médical

- Conserver 10 ans après consolidation

Certains fichiers de gestion du personnel

- Conserver jusqu'à liquidation des droits à la retraite

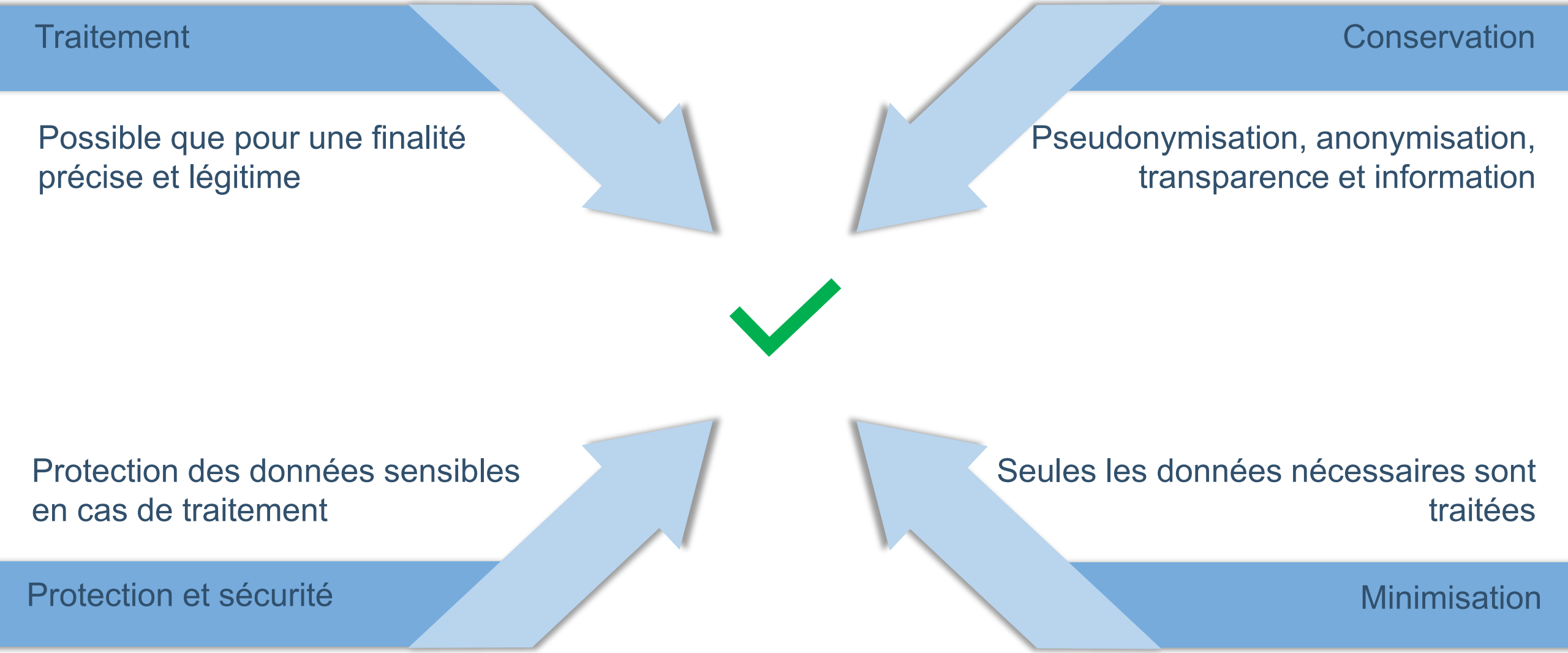
Images de vidéosurveillance

- Conserver 1 mois après la capture sauf instruction

Données de prospection (non client)

- Conserver 3 ans après dernier contact

RGPD – LES GRANDS PRINCIPES



PRINCIPES DE PROTECTION DES DONNÉES – EXEMPLES CONCRETS

- Case de consentement pour un formulaire ou l'utilisateurs renseigne des données qui ont vocation à être stockées et utilisées
- Bouton obligatoire de désinscription lors de l'envoie d'une newsletter
- La demande de suppression des infos en BDD (droit à l'oubli)
- Si le site en utilise : le consentement aux cookies

RGPD – EXERCICE

Réalisez une étude de cas en vous inspirant des sujets suivants :

https://blockproof.fr/blog/sanctions-rgpd-entreprises-pays

Objectif :

Recensez et expliquez les erreurs réalisées par ces entreprises.

Proposez des solutions permettant de pallier les erreurs, d'éviter les sanctions.

RGPD – WOOCLAP

MÉTHODE PDCA

MÉTHODE PDCA – PLAN DO CHECK ACT ou ROUE DE DEMING

1. **Plan**
   Désigner un pilote pour la gouvernance des données ; **Cartographier** vos traitements de données personnelles ; **Prioriser** les actions à mener.
2. **Do**
   Application du plan.
3. **Check**
   Contrôle et identification des traitements susceptibles d'engendrer des risques pour les droits et libertés.
   Une analyse d'impact relative à la protection des données (AIPD) :
   https://www.cnil.fr/fr/gerer-les-risques
4. **Act**
   Appliquer des corrections et revenir au point 1 après des corrections puis documenter la conformité

MÉTHODE PDCA

SÉCURITÉ DES APPLICATIONS – JOUR 2 & 3
COMMUNICATION DU PLANNING

- Correction de l’exercice 1, commentaires et exemple (Plan de sensibilisation EPSI)
- Rendu de l’exercice 2 (Étude de cas RGPD) attendu pour vendredi soir 20h, non noté.
- QCM vendredi 10h, sur ce qui a été vu lundi et aujourd'hui (jeudi).
- Coding d’exemples de failles SQLI, XSS, CSRF et RFI.
  - à déposer sur votre repo (gitlab, github, bitbucket).
  - M’envoyer le lien du repo par mail, exemple : https://github.com/tvinchent-epsi

ORGANISATION DU MODULE

Jour 1 (lundi)

Généralités + exercice

RGPD & Principes de protection des données

Jour 2 (jeudi)

Failles communes

TP : Injection SQL (Python & PHP)

Jour 3 (vendredi)

Failles communes (suite)

TP : XSS, CSRF, RFI (PHP)

Failles communes

4 PRINCIPALES FAILLES

1. SQLI : un envoie de donnée non fiable à un interpréteur dans le cadre d'une commande ou d'une requête
2. XSS : une inclusion de donnée non fiables dans une page web sans validation ou échappement approprié
3. CSRF : un envoie à une personne ayant des droits d'une adresse permettant d'effectuer des actions sur la base de donnée
4. RFI : une inclusion d'un fichier externe permettant l'affichage des variables de la page contenant des accès (mot de passe etc.)

FAILLES COMMUNES – OWSAP TOP TEN

TOP 10 WEB APPLICATION SECURITY RISKS

1. **Injection SQL**
2. Broken Authentication
3. Exposition de données sensibles
4. XML Entités externes (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. **Cross-Site Scripting XSS**
8. **Cross Site Request Forgery CSRF**
9. **Local Remote File Inclusion RFI**
10. Insecure Deserialization
11. Using Components with Known Vulnerabilities
12. Insufficient Logging & Monitoring
13. Attaque par force brute et dictionnaire

FAILLES COMMUNES – OWSAP TOP TEN

TOP 10 WEB APPLICATION SECURITY RISKS

1. Injection SQL

Les failles d'injection, telles que l'injection SQL, NoSQL, OS et LDAP, se produisent lorsque des données non fiables sont envoyées à un interpréteur dans le cadre d'une commande ou d'une requête.
Les données hostiles de l'attaquant peuvent inciter l'interpréteur à exécuter des commandes non souhaitées ou à accéder à des données sans autorisation appropriée.

2. Broken Authentication

Les fonctions d'application liées à l'authentification et à la gestion des sessions sont souvent mises en œuvre de manière incorrecte.

3. Exposition de données sensibles

De nombreuses applications Web et API ne protègent pas correctement les données sensibles, telles que les données financières, les données de santé et les informations nominatives.

TOP 10 WEB APPLICATION SECURITY RISKS

~~4. XML Entités externes (XXE)~~

~~De nombreux processeurs XML anciens ou mal configurés évaluent les références aux entités externes dans les documents XML.~~

5. Broken Access Control

Les restrictions sur ce que les utilisateurs authentifiés sont autorisés à faire ne sont souvent pas correctement appliquées.

6. Security Misconfiguration

La mauvaise configuration de la sécurité est le problème le plus fréquemment rencontré.

FAILLES COMMUNES – OWSAP TOP TEN

TOP 10 WEB APPLICATION SECURITY RISKS

7. **Cross-Site Scripting XSS**

   Les failles XSS se produisent lorsqu'une application inclut des données non fiables dans une nouvelle page Web sans validation ou échappement approprié, ou met à jour des données fournies par l'utilisateur en utilisant une API en HTML ou en JavaScript.

8. **Cross Site Request Forgery CSRF**

9. **Local Remote File Inclusion RFI**

10. **Insecure Deserialization**

    Une désérialisation non sécurisée conduit souvent à l'exécution de code à distance.

    Hashage des mots de passe.

    Exemple NTCS JS. (les contrôles en JS peuvent être désactivés). Mais il faut les mettre quand même, pourquoi ?

11. **Using Components with Known Vulnerabilities**

    Les composants, tels que les bibliothèques, les frameworks et autres modules logiciels, s'exécutent avec les mêmes privilèges que l'application.

12. **Insufficient Logging & Monitoring**

    Une journalisation et une surveillance insuffisantes, associées à une intégration manquante ou inefficace avec la réponse aux incidents

13. Attaque par force brute et dictionnaire

    Utilisation des mots de passes les plus courants ou issus de base de données piratée

FAILLES COMMUNES – LES DIFFÉRENTS TYPES D'ATTAQUANT

Le salarié / stagiaire

Opportuniste et avec peu de ressources.

Le concurrent

Intérêts financiers, mais de faibles moyens.

Le crime organisé

Intérêts financiers, et des moyens conséquents.

Les états

Intérêts politiques et économiques et avec des moyens illimités.

INITIATION À ROOT-ME

https://www.root-me.org/

section « challenge / web – client »

FAILLES COMMUNES – EXEMPLE D'UNE INJECTION SQL CLIENT

1. Le pirate saisit une requête SQL dans le champ Login et dans le champ mot de passe. Par exemple : X' or '1'='1

2. Le pirate lance la requête via le bouton de connexion.

3. La requête s'exécute, le pirate est authentifié en tant qu'admin et a accès sans restriction au site.

FAILLES COMMUNES – EXEMPLE D'UNE INJECTION SQL SERVEUR

1. Le pirate saisit une requête SQL dans le champ Login et ne saisit aucun mot de passe. Par exemple :
   $query = "SELECT * FROM USERS WHERE username = '".$_GET['username']."' AND password = '".$_GET['password']."' LIMIT 1;";

2. Le pirate lance la requête via le bouton de connexion.

3. La requête s'exécute, le pirate est authentifié en tant qu'admin et a accès sans restriction au site.

FAILLES COMMUNES – INJECTION SQL SERVEUR – EXERCICE PYTHON

- # Créer une fonction qui retourne si l'utilisateur est admin ou non
- En allant chercher l'information en base de donnée

FAILLES COMMUNES – INJECTION SQL SERVEUR – EXERCICE PHP

- **Construire un formulaire d'identification de la manière la plus simple possible, mais bien sûr fonctionnelle**
- Si pas déjà fait : installez Apache MySQL et PHP sur votre machine (avec par exemple WAMP)
- Créez une base de données avec une table 'user' avec un enregistrement
- Créez une page, contenant :
  - un formulaire d'identification
  - une requête à la base de données pour vérifier si le couple login/pwd existe
  - retourne un résultat « utilisateur reconnu / non reconnu »

FAILLES COMMUNES – EXEMPLE CROSS-SITE SCRIPTING

Injecter du code client tel que du Javascript ou même de l'HTML dans une ressource distante

- Persistant : Le code injecté va être stocké dans une base de données (la base de données utilisée par l'application).

- Non persistant : Le code ne sera pas stocké et ne pourra être réutilisé que si la personne malveillante le réinjecte sur un site (Article posté par un Utilisateur).

FAILLES COMMUNES – EXEMPLE CROSS-SITE SCRIPTING

1. Au lieu d'écrire le champ de saisie de l'article, le pirate saisit dans le champ texte le code suivant :

```
<script>document.location="http://www.monSiteMalveillant.com" </script>
```

2. Le pirate poste l'article.

3. Lorsqu'un utilisateur consultera la page de l'article, le code s'exécutera et un Utilisateur du site sera redirigé sur l'adresse.

FAILLES COMMUNES – EXEMPLE CROSS-SITE SCRIPTING

1. Dans la barre de recherche, le pirate saisit par exemple :

   `<script>alert(1);</script>`

2. Le pirate lance la recherche.

3. L'alerte affichant, par exemple, une pop-up avec comme contenu « 1 » apparait sur l'écran.

FAILLES COMMUNES – CROSS-SITE SCRIPTING - EXERCICE

- **Construire un livre d'or de la manière la plus simple possible, mais bien sûr fonctionnelle**
- Créez une base de données avec une table 'livredor'
- Créez une page, contenant :
  - un affichage des entrées du livre d'or
  - un formulaire pour ajouter un mot au livre d'or
  - l'insertion de ce mot en cliquant sur le bouton d'envoie

FAILLES COMMUNES – EXEMPLE CROSS-SITE SCRIPTING

ROOT ME

Premier pas avec Javascript

https://www.root-me.org/en/Challenges/Web-Client/Javascript-Source
https://www.root-me.org/en/Challenges/Web-Client/Javascript-Authentication

Exercice Cross-Site Scripting

https://www.root-me.org/fr/Challenges/Web-Client/XSS-Stored-1

FAILLES COMMUNES – EXEMPLE
CROSS-SITE REQUEST FORGERY (**CSRF**)

Type de menace web qui manipule le navigateur web pour qu'il effectue une action non désirée sur l'application ou le site web auquel un utilisateur est actuellement connecté.

1. Une demande de virement d'une banque est falsifiée et le lien est intégré à un courriel ou à un site Web.
2. L'utilisateur clique sur le lien sans se méfier.
3. La banque reçoit la requête et réalise le virement depuis le compte de l'Utilisateur vers celui du pirate.

FAILLES COMMUNES – EXEMPLE
CROSS-SITE REQUEST FORGERY (**CSRF**)

Illustration de faille CSRF en PHP

FAILLES COMMUNES – EXEMPLE
CROSS-SITE REQUEST FORGERY (**CSRF**)

ROOT ME

https://www.root-me.org/fr/Challenges/Web-Client/CSRF-0-protection

FAILLES COMMUNES – EXEMPLE
LOCAL REMOTE FILE INCLUSION

L'inclusion de fichiers à distance est une vulnérabilité que l'on trouve souvent dans des applications Web mal écrites

1. Le pirate injecte un script dans une application Web.
2. Le script est exécuté sur le serveur Web.
3. Le serveur télécharge le script malicieux depuis le site Web du pirate.
4. Le pirate prend le contrôle à travers l'application Web.

FAILLES COMMUNES – EXEMPLE
LOCAL REMOTE FILE INCLUSION

Illustration de faille RFI en PHP

FAILLES COMMUNES – EXEMPLE
LOCAL REMOTE FILE INCLUSION

ROOT ME

- Pour la réalisation de ce challenge, il est recommandé de le faire depuis une machine virtuelle.

https://www.root-me.org/fr/Challenges/Web-Serveur/Remote-File-Inclusion

FAILLES COMMUNES – WOOCLAP

APT

QU'EST-CE QU'UNE ATTAQUE APT ?

- Advanced Persistent Threat
- Une catégorie d’attaques mettant en œuvre de nombreuses techniques d’attaques (injection SQL, XSS, etc.)
- AET (Advanced Evasion Techniques) qui est une technique dite d’évasion

ADVANCED PERSISTENT THREAT

- Attaque dite avancée dans le sens qu'elle utilise toutes les techniques et outils pour atteindre son objectif
- Multitude de composants communs
- L'ensemble des méthodes et outils font d'elle une attaque avancée

ADVANCED **PERSISTENT** THREAT

- Attaque basée sur la stratégie de rester le plus longtemps possible
- Scénarisée par les attaquants
- Objectif : rester sous les radars

ADVANCED PERSISTENT **THREAT**

- Coordination de moyens techniques et humains
- Peu automatisé
- Techniques inhabituelles

PARTICULARITÉS DES APT

- Utilisent les mêmes vecteurs d’attaques que les attaques traditionnelles
- Ne cherchent pas systématiquement à exploiter une vulnérabilité
- Le facteur humain est plus souvent utilisé
- Mettent rarement en œuvre des attaques de type « déni de service » ou des « defacements »

COMMENT S’EN PROTÉGER ?

- Maintien des systèmes à jour
- Sensibilisation des utilisateurs
- Sensibiliser les HelpDesks face à des anomalies récurrentes
- Préparation des administrateurs (remontée de logs ou anomalies)

DEVOIR

Choisissez une attaque APT dans la liste https://fr.wikipedia.org/wiki/Advanced_Persistent_Threat

- explication de l'exploit ? (3pts)
- comment s'en protéger ? (4pts)
- L'impact politique / économique ? (2pts)

Document à rendre contenant au maximum 2 pages

Rendu en groupe de minimum 2 personnes