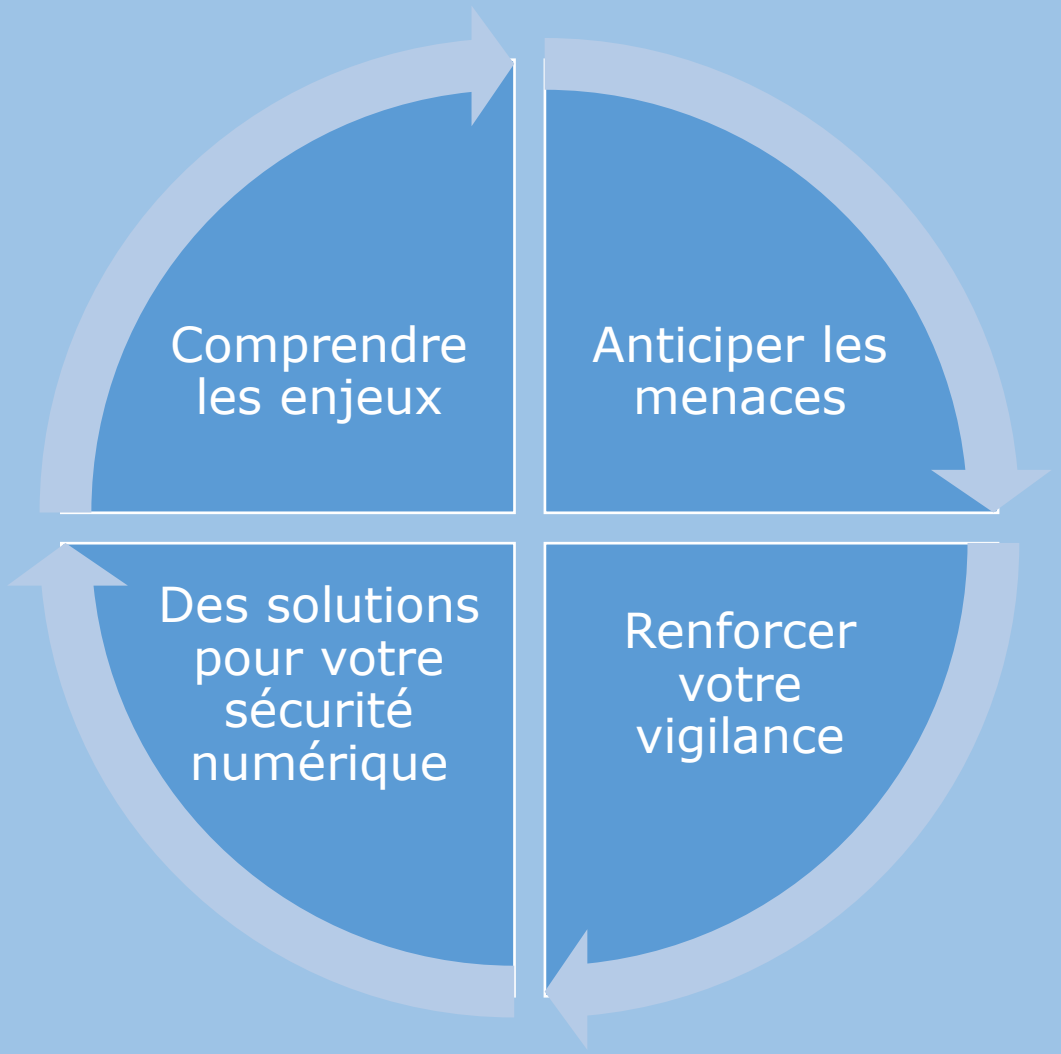
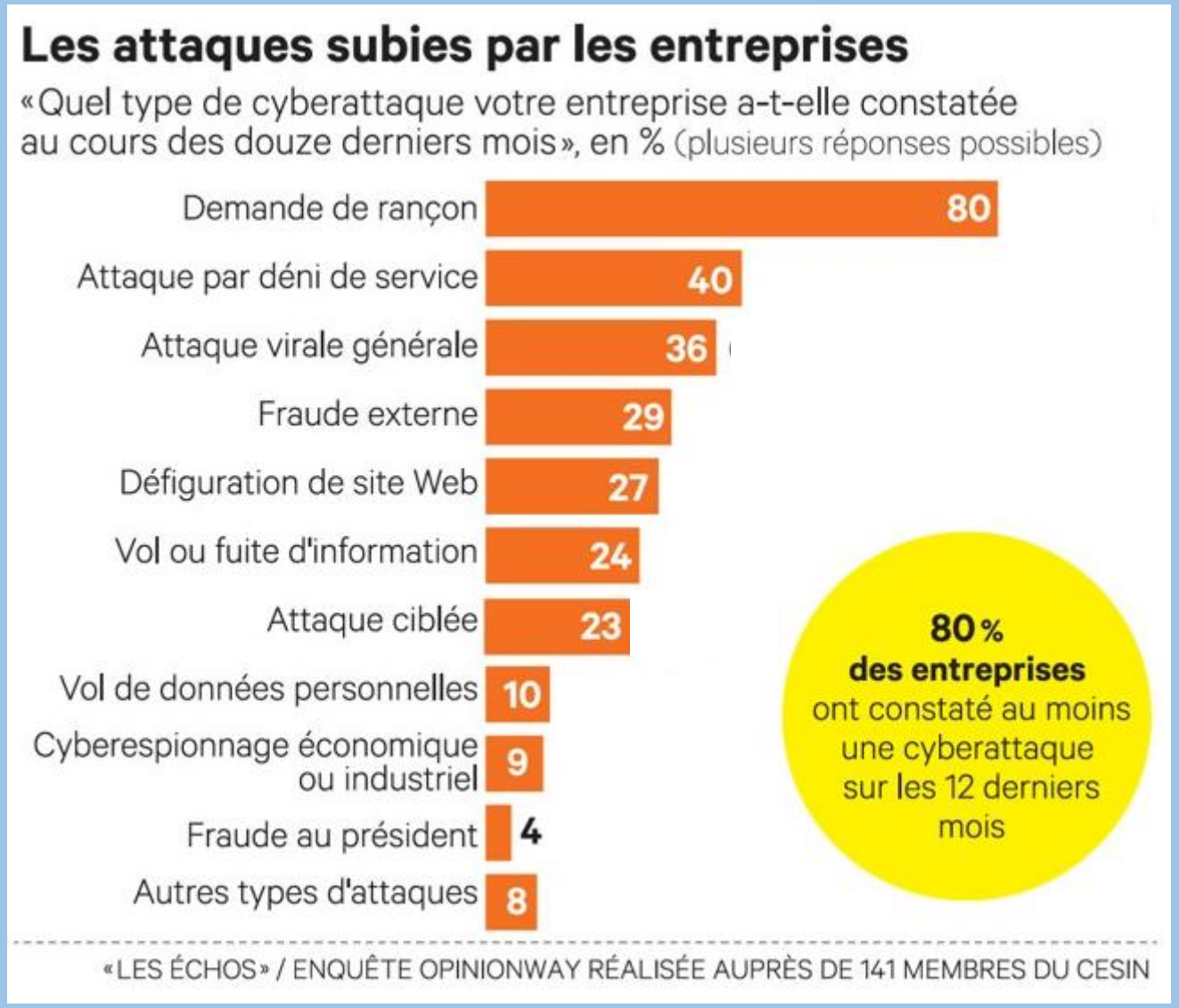
Sensibilisation à la sécurité numérique

Objectif : sensibiliser à la sécurité numérique

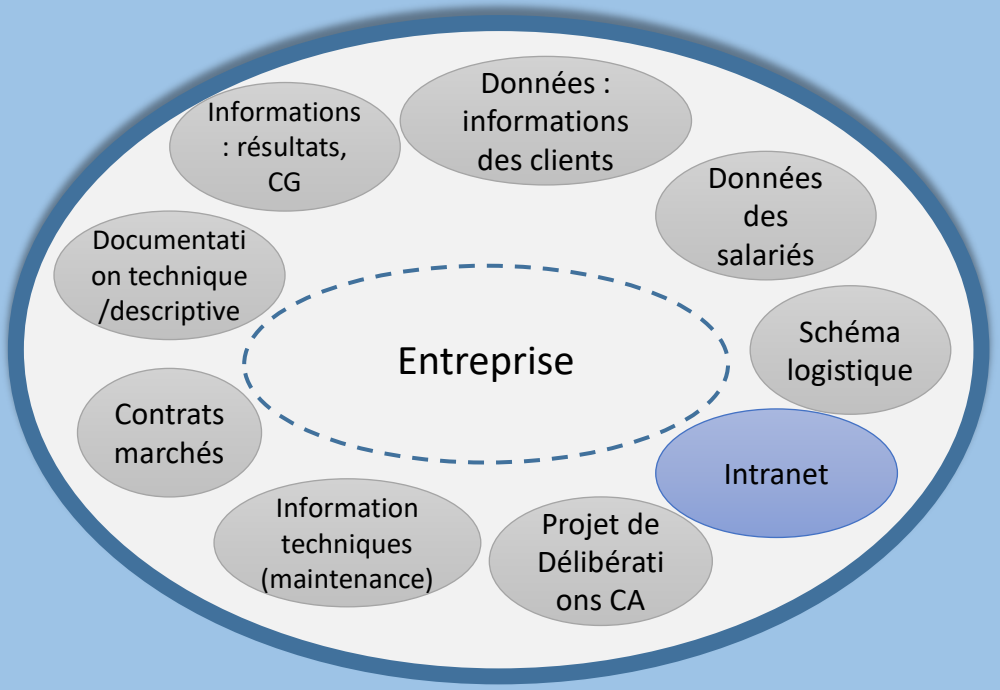


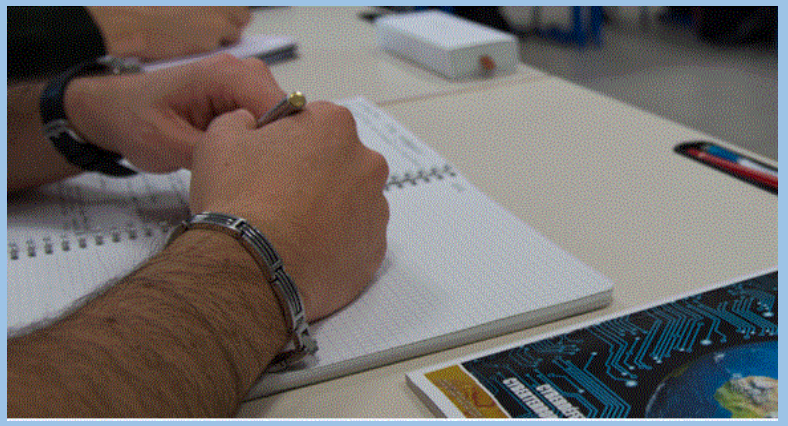
EXEMPLES :


Les attaques subies par les entreprises
«Quel type de cyberattaque votre entreprise a-t-elle constatée au cours des douze derniers mois», en % (plusieurs réponses possibles)
Demande de rançon 80
Attaque par déni de service 40
Attaque virale générale 36
Fraude externe 29
Défiguration de site Web 27
Vol ou fuite d'information 24
Attaque ciblée 23
Vol de données personnelles 10
Cyberespionnage économique ou industriel 9
Fraude au président 4
Autres types d'attaques 8
80 % des entreprises ont constaté au moins une cyberattaque sur les 12 derniers mois
«LES ÉCHOS» / ENQUÊTE OPINIONWAY RÉALISÉE AUPRÈS DE 141 MEMBRES DU CESIN

COMPRENDRE LES ENJEUX des PME

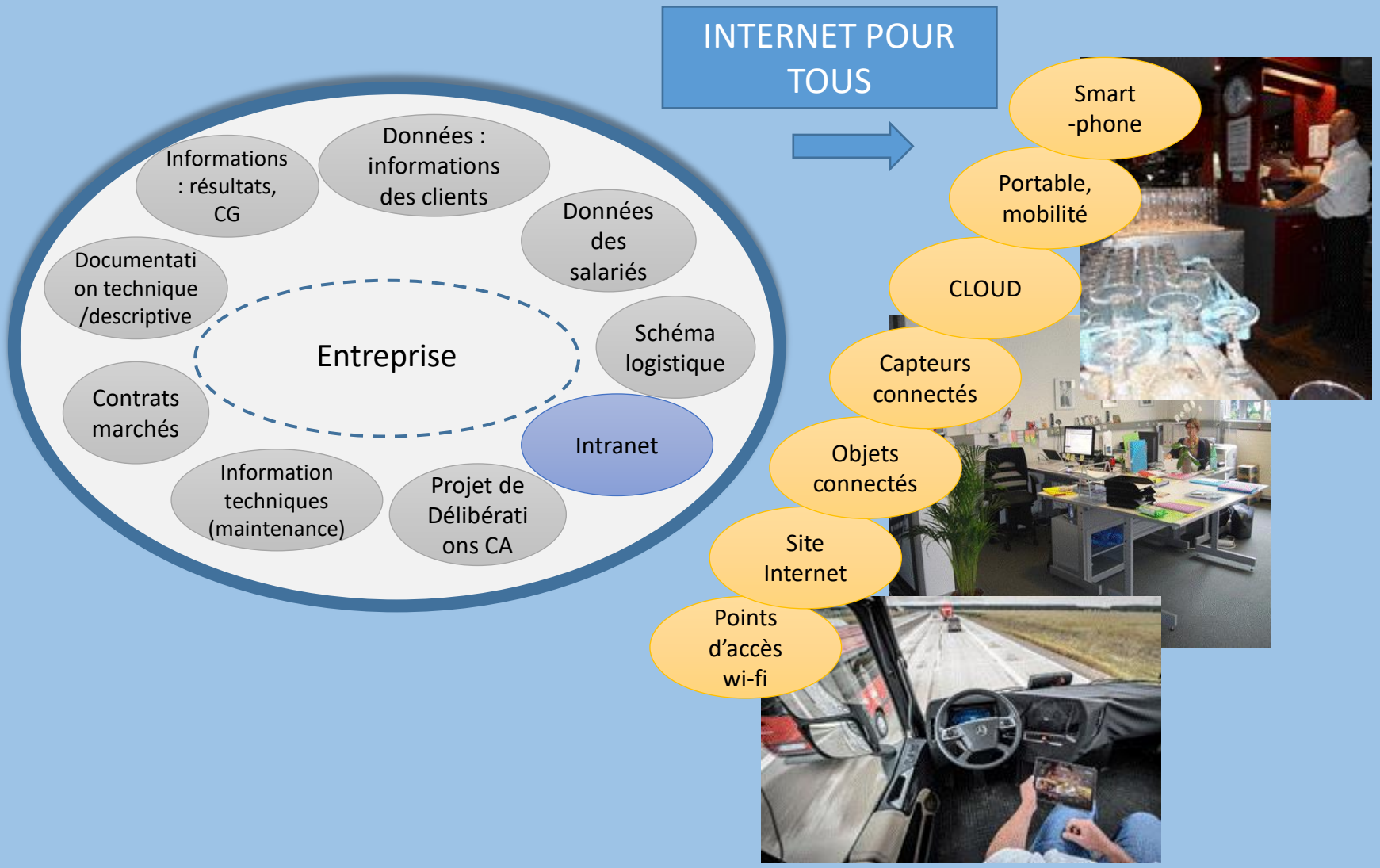
LE MONDE CHANGE





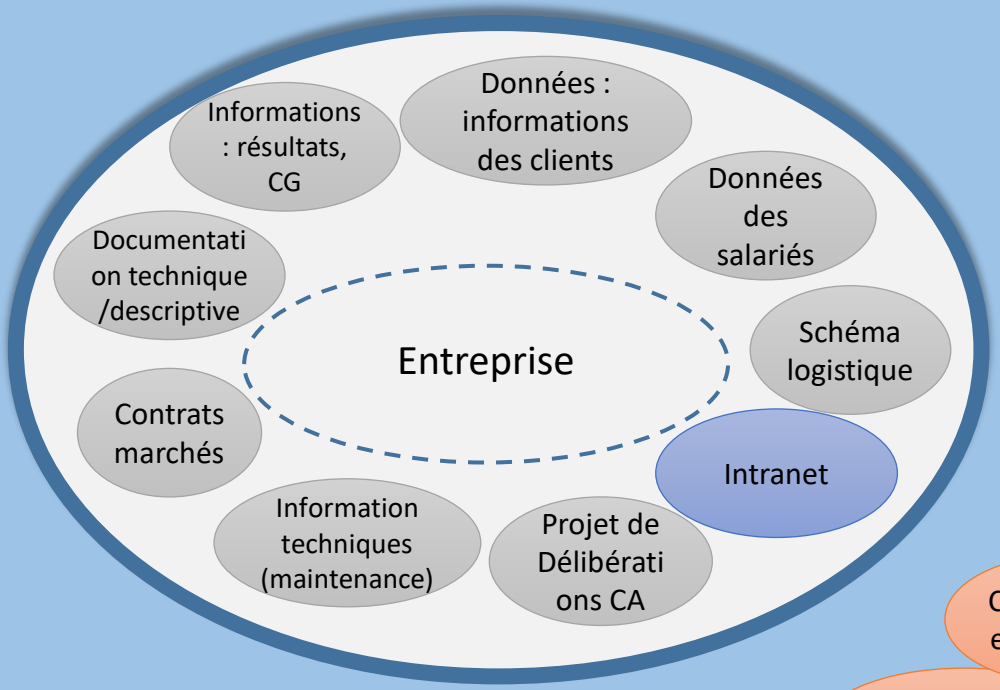
COMPRENDRE LES ENJEUX des PME

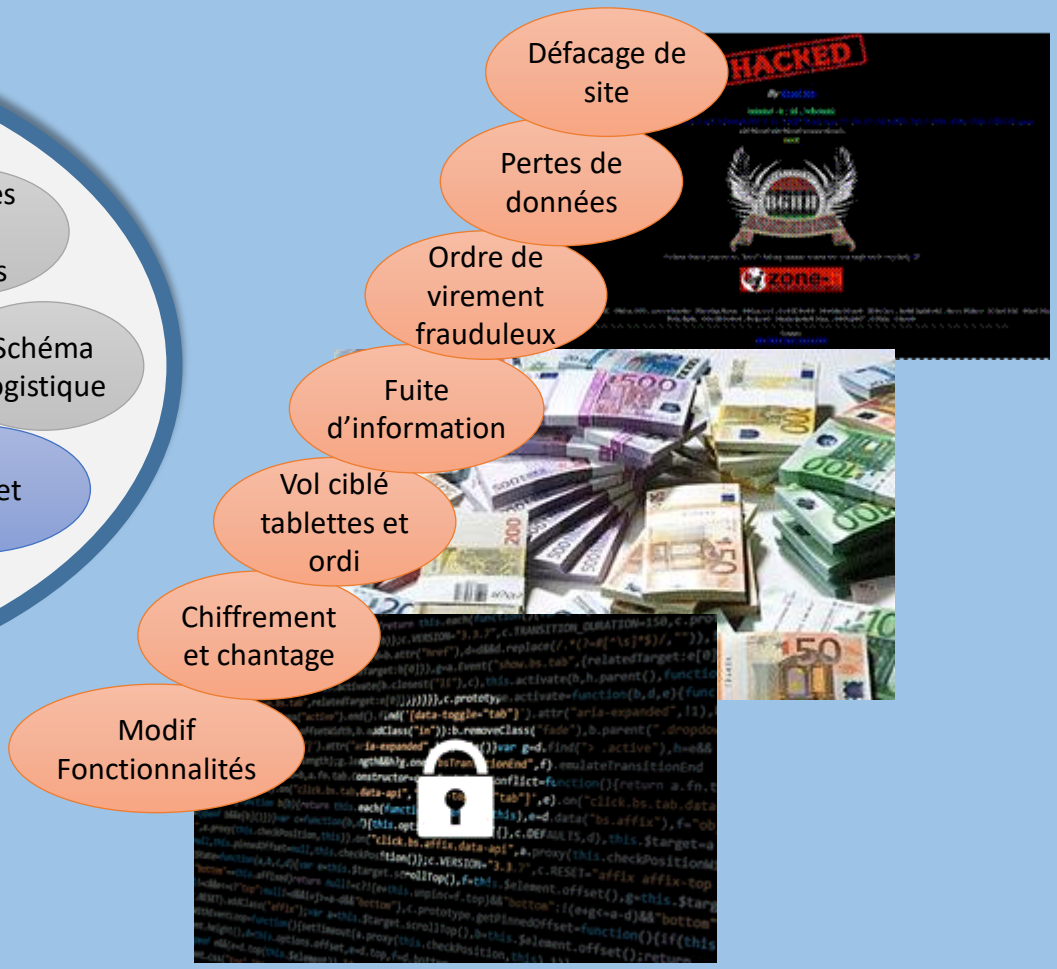
LE MONDE CHANGE



COMPRENDRE LES ENJEUX des PME

LE MONDE A CHANGE

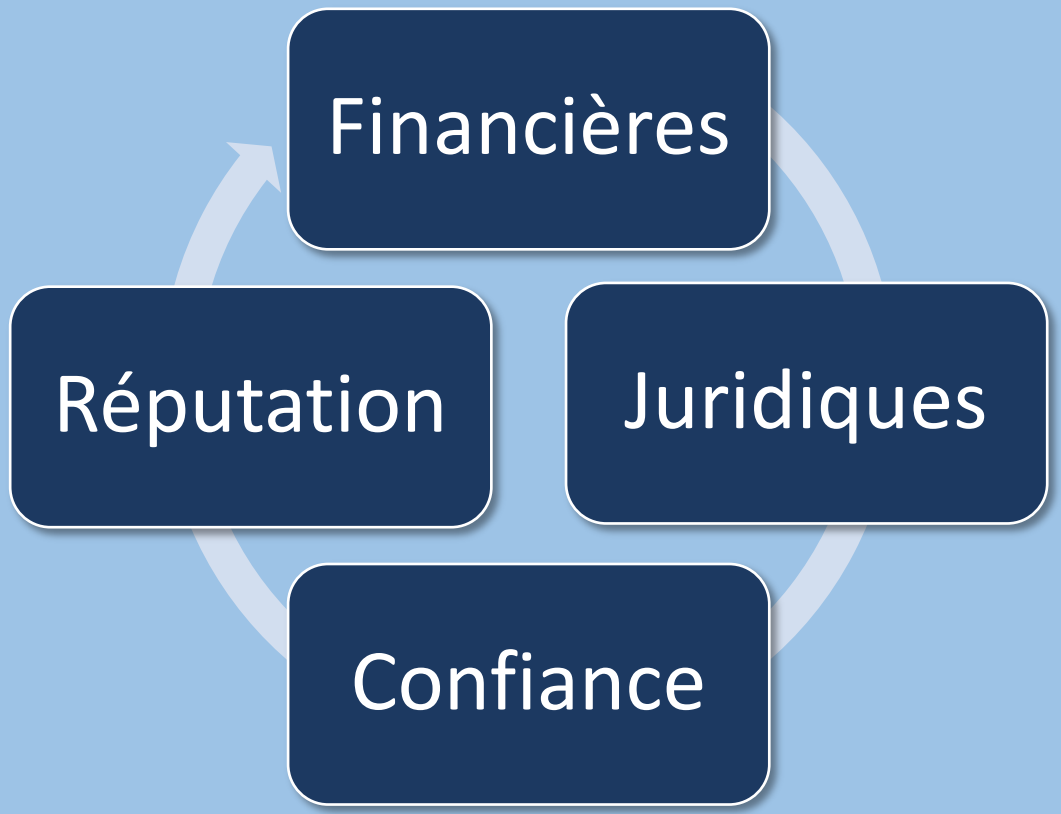




COMPRENDRE LES ENJEUX POUR LES PME

Conséquences

En quoi la sécurité des entreprises est-elle importante ?



ANTICIPER LES MENACES

Motivation des attaquants

LUCRATIVE
Bandes organisées
Individus

TECHNIQUE
Hacker

LUDIQUE
Adolescent geek

ETAT
Unités spécialisées

POLITIQUE
Hacktivistes
Cyberpatriotes
Cyberterroristes

Vengeance / vindicte
Employé mécontent
Intérêts individuels

ANTICIPER LES MENACES

L'humain

Malveillance et fraude interne

Les attaques proviennent également de l'interne :
le départ de salariés, ou l'accueil de stagiaires peuvent être des situations à risques

LES EMPLOYÉS QUITTENT LEUR ENTREPRISE EN EMPORTANT DES DONNÉES AVEC EUX

Publié le 16/07/2012 par **Laurent Bailliard**

Propositions commerciales, plans stratégiques, feuilles de route de produits/services... Autant d'informations qui quittent l'entreprise lors des départs de salariés. De quoi mettre à mal la compétitivité de l'entreprise.

Détournement de données de l'entreprise, condamnation d'un salarié pour abus de confiance

EXEMPLES : RANSOMWARE

Hacké et rançonné : DOMINO'S PIZZA, juin 2014, fichier de 600 000 clients avec mot de passe, demande de rançon de 30 000 Euros

Hacké et rançonné : NOKIA en 2008, code source des téléphones portables, demande de rançon plusieurs Millions d'Euros

….


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

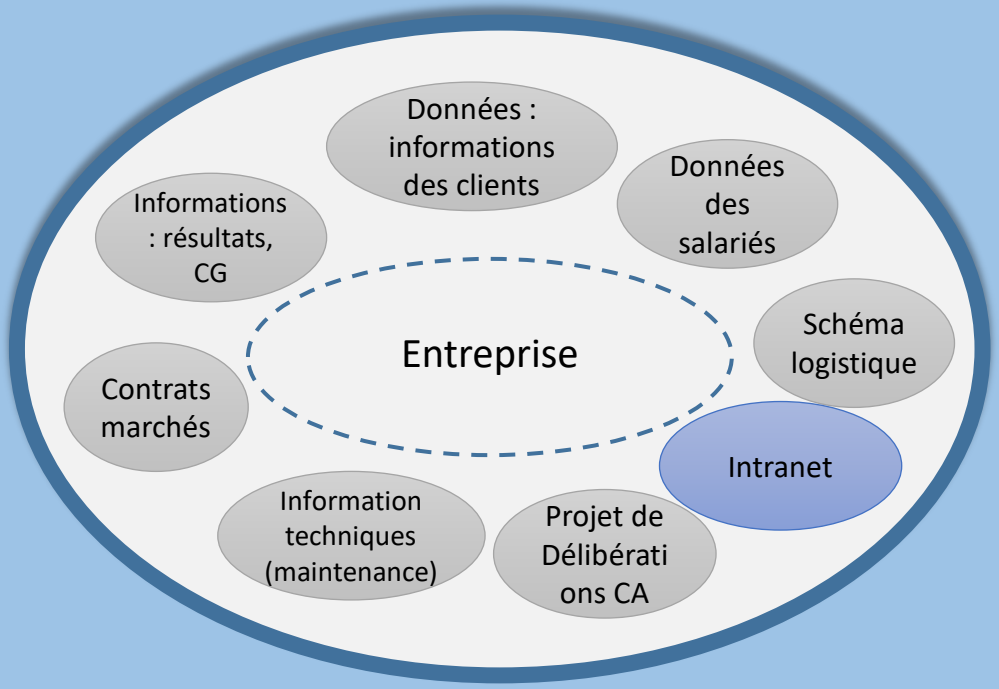
EXEMPLES : ingenierie sociale

Ingénierie sociale : Virement frauduleux (Reims). Incroyable mais vrai ! Se faisant passer pour le patron d'une PME rémoise, un escroc a envoyé à sa banque un faux ordre de virement de 88 700 € sur un compte de la Bank of China.

….

RENFORCER LA VIGILANCE

Identifier les objets à risques ou porteurs de valeur…



Données confidentielles : stratégiques, Personnelles…

Données INTERNES

Données publiques

… et les protéger en priorité !

DES SOLUTIONS

Une question de bon sens

3 Axes

- Comportemental
- Organisationnel
- Technique

«L'épaisseur d'un rempart compte moins que la volonté de le défendre»

Citation de Thucydide
historien grec 5ème
Siècle avant J.C.

DES SOLUTIONS

COMPORTEMENT : Sensibiliser

Écran non verrouillé

Mot de passe inscrit sur un post-it

Utilisation d'outils personnels (Smartphones, clés…)

Risque d'ingénierie sociale

Documents non rangés

Documents non détruits

Qui contacter…

…en cas de cyberattaque ?

Il faut déposer plainte auprès d'un service de Police Nationale ou de Gendarmerie Nationale

Sur Paris, 92, 93 et 94

Contacter la BEFTI (Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information)

01 55 75 26 19

Pppj-befti-information@interieur.gouv.fr

Partout en France

Se rapprocher des services locaux de l' Police Nationale ou de l' Gendarmerie Nationale

http://www.police-nationale.interieur.gouv.fr

http://www.gendarmerie.interieur.gouv.fr

cybermalveillance.gouv.fr

Pour plus d'informations :
http://www.ssi.gouv.fr/en-cas-dincident

L’hygiène informatique

Comment se protéger ?

1- Mots de passe : faites preuve d'imagination

2- Mises à jour : ~~je le ferai demain!~~

3- Privilèges : à quoi bon avoir tous les droits

4- Sauvegardes : l'atout sérénité

5-Wi-fi, clés USB, ETC. : N'ouvrez pas la porte à n'importe qui

6-Ordinateur, téléphone, tablette : même combat !

7-Nomadisme : faites rimer mobilité et sécurité

8-Messagerie : méfiez-vous des apparences…

9-Téléchargements : gare aux arnaques !

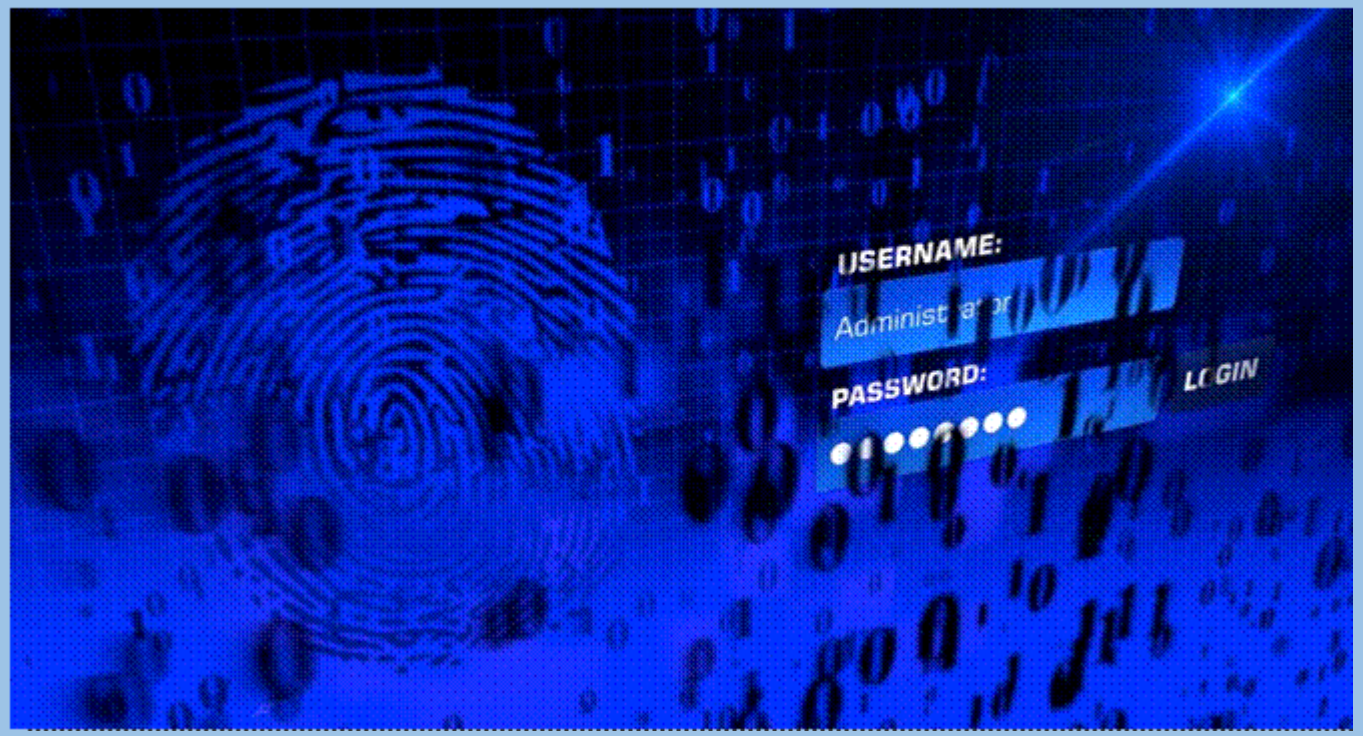
10-Paiement en ligne : évitez les frais

11-Séparation des usages : un jeu d'enfant ?

12-Identité numérique : attention dossier

Guide des bonnes pratiques

1. Choisir avec soin ses mots de passe



Guide des bonnes pratiques

2. Mettre à jour régulièrement vos logiciels

9. Télécharger ses programmes sur les sites officiels des éditeurs

Guide des bonnes pratiques

4. Effectuer des sauvegardes régulières

Plan de reprise d'activité

Guide des bonnes pratiques

6. Être très prudent avec son smartphone

11. Séparer les usages personnels des usages professionnels

Guide des bonnes pratiques

12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Sécurité numérique

Questions - Réponses