



WEBINAIRE

TPE-PME, Ne laissez pas la cybermalveillance menacer votre reprise !

LA CPME EST LA PREMIÈRE ORGANISATION INTERPROFESSIONNELLE
À ÊTRE CERTIFIÉE ENGAGEMENT DE SERVICE QUALI'OP



PROGRAMME

- **La protection cyber, notion indissociable de celle de transition numérique**

Alain Assouline, CPME, Président de la commission numérique

- **Les actions de la CPME, les risques et attaques touchant principalement les TPE et PME, le darkweb**

Marc Bothorel, CPME, Référent cybersécurité

- **Les conseils de protection cyber et leur mise en œuvre au sein de l'entreprise**

Daniel Benabou, Conseil de l'économie et de l'information du digital, Co-président

- **Questions/réponses**

Elles devront être rédigées dans l'onglet « questions »

INTRODUCTION

La protection
cyber, notion
indissociable de
celle de transition
numérique

Alain Assouline

CPME,
Président de la
Commission numérique

Les actions de la
CPME,
Les risques et
attaques touchant
principalement les
TPE et PME,
Le darkweb

Marc Bothorel

CPME,
Référent cybersécurité

TELETRAVAIL, COVID, CRISE ECONOMIQUE : UNE MANNE POUR LES CYBERCRIMINELS !



10To de données volées



Rançon 8M Euros



3 mois de remise en état



Fermeture des serveurs
Arrêt des sites de production



550 Millions de comptes piratés dont 20 millions de français (nom, prénom, adresse, tel mobile, compte mail etc.)
Avril 2021



500 millions de comptes piratés en vente sur le DarkWeb
Avril 2021



Business Services

339Mo données
20 clients touchés



Rançonné +15 jours sans accès dossiers client
Avril 2021



« On croit toujours que l'on a un antivirus à toute épreuve. Pour ma part, je me croyais à l'abri mais aujourd'hui, les pirates sont plus organisés que les entreprises et les virus plus dangereux qu'on ne le croit »⁽¹⁾

⁽¹⁾ Article du Télégramme du 15 Juillet 2020

Vecteurs d'attaque :

Grande sociétés → ingénierie sociale, phishing
PME → principalement les failles RDP/RDS, phishing

QUELQUES CHIFFRES SUR L'ACTIVITÉ CYBERCRIMINELLE EN 2020 (FRANCE)

Les cyberattaques ont explosé en 2020

LA CYBERCRIMINALITÉ X4
L'ANSSI indique avec triste surprise le plus d'attaques de rançongiciels en 2020, par rapport à l'année précédente. Ces données qui ont fortement augmenté à partir de septembre, ne concernent que les cas où elles a été assenée à l'intérieur (Etat, administrations, opérateurs d'importance vitale).

2019

2020

Une autre menace qui n'est pas nouvelle et bien réelle, à laquelle il ne serait pas vraiment accordé suffisamment d'attention :
L'ESPIONNAGE



LES RANÇONGICIELS*

Selon les données du GIP ACYMAP®, les cyberdélinquants se sont réorientés en 2020 vers des cibles potentiellement les plus lucratives :

LES PARTICULIERS
sont moins ciblés, leurs appels à l'aide se sont réduits :
2972 → 401

LES ENTREPRISES
ayant révélé avoir été touchées en 2019 / 2020
667 → 837

LES COLLECTIVITÉS
ayant révélé avoir été touchées en 2019 / 2020
103 → 159

* AVISEMENT : Les données anonymes sur cette infographie ne sont que le reflet d'événements réels, traités en identités. Celles-ci ne prennent pas en compte les attaques non dévoilées publiquement.

D'AUTRES ATTAKUES PRESQUE SILENCIEUSES
qualifiées de quasi militaires, dont l'objectif n'est pas explicite où l'on cherche à introduire une instabilité dans un pays ou des conflits peuvent présager des conflits futurs.

IS Agence Nationale pour la Sécurité des Systèmes d'Information
GIP ACYMAP : Groupe d'Intelligence Public Action contre la Cybercriminalité
GIPS : Groupe d'Intelligence Public Action contre la Sécurité

Nomeshield group

LES CYBERATTAQUES EN 2020 EN CHIFFRES

94 %

des responsables sécurité interrogés ont déclaré avoir été la cible d'une cyberattaque en 2020

Selon Deloitte Forecast "The Rise of the Business-aligned Security Executive - 2020"

LES ENTREPRISES QUI ONT SUBI UNE CYBERATTAQUE DÉCLARENT :



38%
ont connu une perte de productivité

33%
ont perdu des données clients

32%
ont perdu des données salariés



des TPE / PME qui ont connu une attaque majeure ont cessé leur activité dans les 6 mois suivants

Selon Accenture Security en 2018

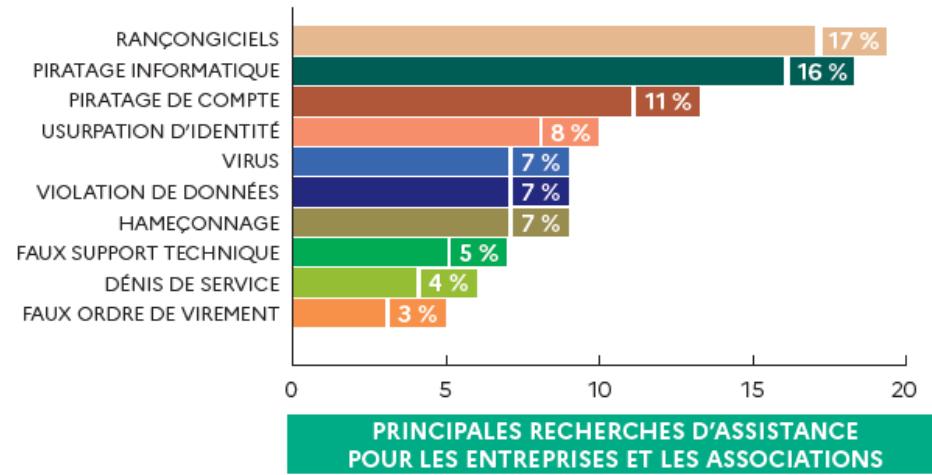
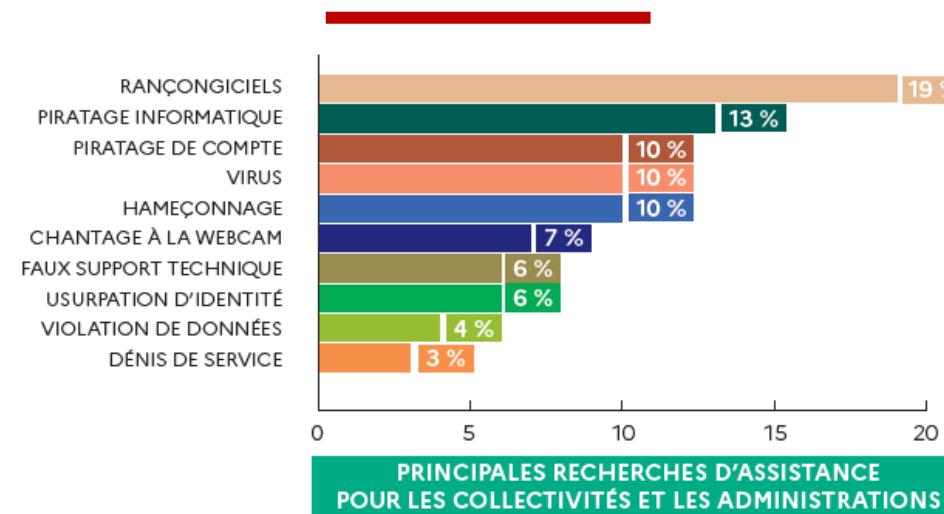
10 000 à 100 000€

c'est le coût variable que représente une cyberattaque pour les PME françaises

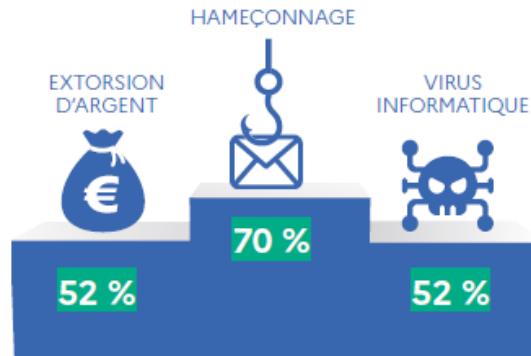
almeria
solutions informatiques



QUELS SONT LES PRINCIPAUX ACTES DE CYBERMALVEILLANCE EN 2020 EN FRANCE¹?



3 actes de cybermalveillance le plus souvent rencontrés en 2020 en France



*Rapport
cybermalveillance.gouv.fr 2020

INCIDENTS CYBER EN 2019/2020 ET PROJECTIONS 2025

CYBERCRIMINALITÉ EN FRANCE⁽³⁾

En 2018, 80% des entreprises ont constaté un incident de cybercriminalité

En 2019, 90 % des entreprises ont constaté un incident de cybercriminalité en France, 43 % étant des PME

En 2020, Ce taux a été multiplié par 4
Le télétravail est devenu la source de 20% des incidents de cybercriminalité



COÛT DE LA CYBERCRIMINALITÉ⁽²⁾

2017 : 600 milliards de dollars

2018 : coût moyen par entreprise a été de 8,6 millions d'euros pour les entreprises françaises.

2021 : 6000 milliards de dollars (190.000 dollars à la seconde) avec pourtant des coûts de mise en œuvre faibles (5 dollars en moyenne pour acheter un virus ou équivalent sur le darknet)

2025 : prévisionnel à 10500 milliards de dollars ce qui, si on devait mesurer le poids du risque cyber en faisant un pays, le positionnerait en troisième économie mondiale derrière les Etats-Unis et la Chine

Sources :

(1) (2) cyberwarfare in the C-suite, Cybersecurity ventures, janvier 2021 et (3)Rapport du ministère de l'Intérieur, État de la menace numérique

Et

Rapport du club des juristes « Le droit Pénal à l'épreuve des cyberattaques » Avril 2021

LES IMPACTS SUR NOS/VOS ENTREPRISES

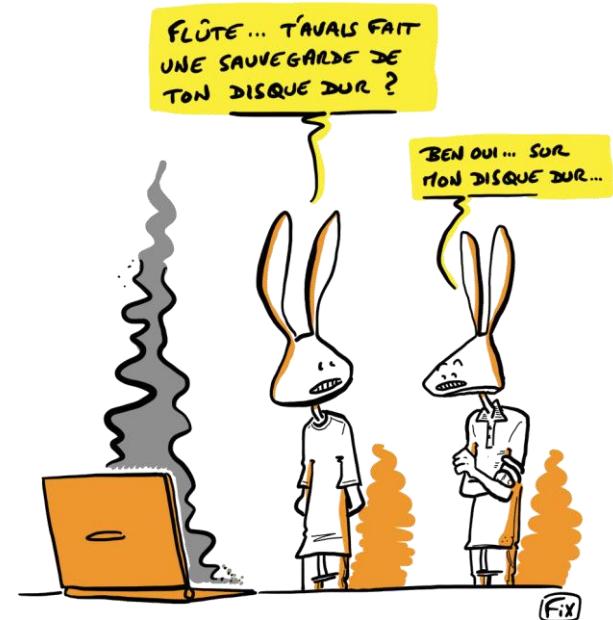
Après annonce d'un cyber incident¹:

- Risque de défaillance augmenté de **80%** dans les 3 mois
- Perte de **8 à 10%** de la valorisation de l'entreprise
- Dommage à la réputation "l'actif immatériel le plus précieux dont dispose l'entreprise »

OR..

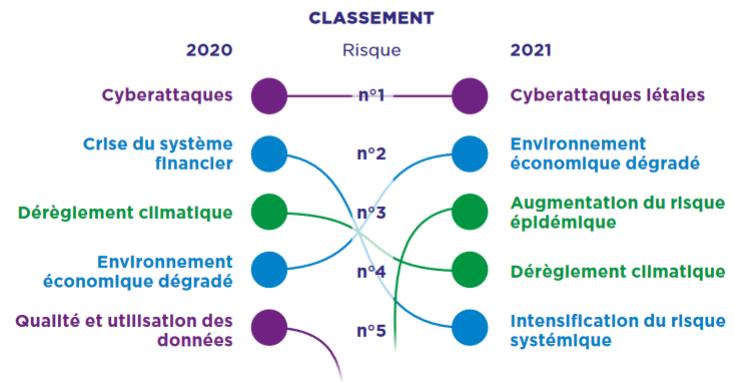
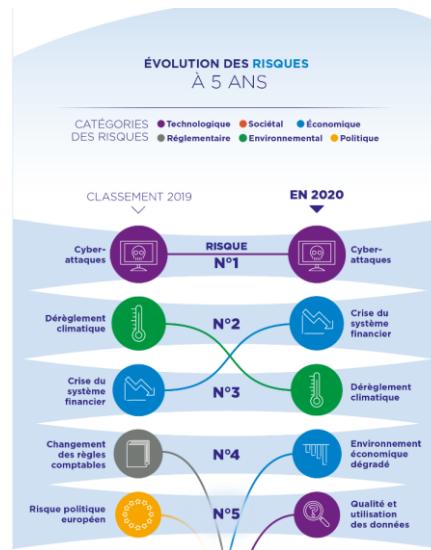
- **80%** des entreprises françaises n'ont pas de plan de réponse aux incidents robustes²
- **86%** des entreprises françaises n'ont pas souscrit à une cyberassurance³

¹: source Etude cabinet Bessé ²: Source IBM Ponemon ³: Source CLUSIF



FFA: BAROMÈTRE 2021 DES RISQUES ÉMERGENTS À 5 ANS

À horizon 5 ans, le principal risque demeure les **cyberattaques létales**, suivi par l'environnement économique dégradé



Source: <https://wwwffa-assurance.fr>

QUELQUES CARTES INTERACTIVES EN TEMPS RÉEL DES CYBERMENACES....

<https://threatmap.checkpoint.com/>

<https://cybermap.kaspersky.com/stats>

<https://threatmap.bitdefender.com/>

<https://www.digitalattackmap.com/>

WEB – DEEPWEB - DARKWEB ???

le deepweb est plus de 500 fois plus gros que le web indexable



Le **deepweb**, ou « web profond », parfois même « web invisible », est souvent défini comme le web accessible mais non indexé par les moteurs de recherche



Le **dark web** désigne le contenu du **World Wide Web** se trouvant sur les **darknets**



On appelle **darknet** les réseaux overlays, à l'origine isolés du réseau public. accessible qu'à l'aide d'outils spécifiques. Les plus connus sont Tor, i2p et Freenet.



LE HACKING, UN VRAI BUSINESS, UNE ECONOMIE PARALLELE

CATEGORIES

- Adult
- Blog
- Carding
- Communication
- Forums
- Hacking
- Hosting
- Markets
- Private Sites
- Search Engines
- Services
- Social
- Wiki/Links
- Other

Best Hacking Services ONLINE 2020-05-09 19:11:22

We have been doing this for years, we know what we do, and we do it fairly well.

[Visit Best Hacking Services](#) + 14 - 72

Hack Facebook and Instagram Account ONLINE 2020-05-09 19:55:42

We sell the cheapest and most reliable Facebook/Instagram hacking service on the deep web.

[Visit Hack Facebook and Instagram](#) + 7 - 38

Darknet Hacking Services ONLINE 2020-05-09 17:43:15

This is an organization and brokerage with a vast network of hacking services tailored to suit each clients needs. Our consulting service provides professional hacking services for hire at your disposal and consists of individuals who have a variety of technical skills to meet each specific request.

Rent-A-Hacker

Rent-A-Hacker

Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my business since I was 16 years old. I never had a real job, so i had the time to get really good at hacking and I made a good amount of money last +20 years.
I have worked for other people before, now I am also offering my services for everyone with enough cash here.

Prices:
I am not doing this to make a few bucks here and there, I am not from some crappy eastern europe country and happy to scam people for 50 EUR.
I am a professional computer hacker who could earn 50-100 EUR an hour with a legal job.
So stop reading this and start a serious problem worth spending some cash at.
Price depends a lot on the problem you want me to solve, but minimum amount for smaller jobs is 250 EUR.
You can pay me anonymously using Bitcoin.

Technical skills:

- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- DDoS, Exploiting, highly personalized trojans, Botnet, DDOS
- Social engineering, getting into your selected targets
- Basically anything a hacker needs to be successful, if I don't know it, I'll learn it very fast
- Anonymity: no one will ever find out who I am or anything about my clients.

Social Engineering skills:

- Very good written and spoken (phone calls) english, spanish and german.
- If I can't hack something technically I'll make phone calls or write emails to the target to get the needed information, I have had people make things you wouldn't believe really often.
- A lot of experience with security practices inside big corporations.

What I'll do:

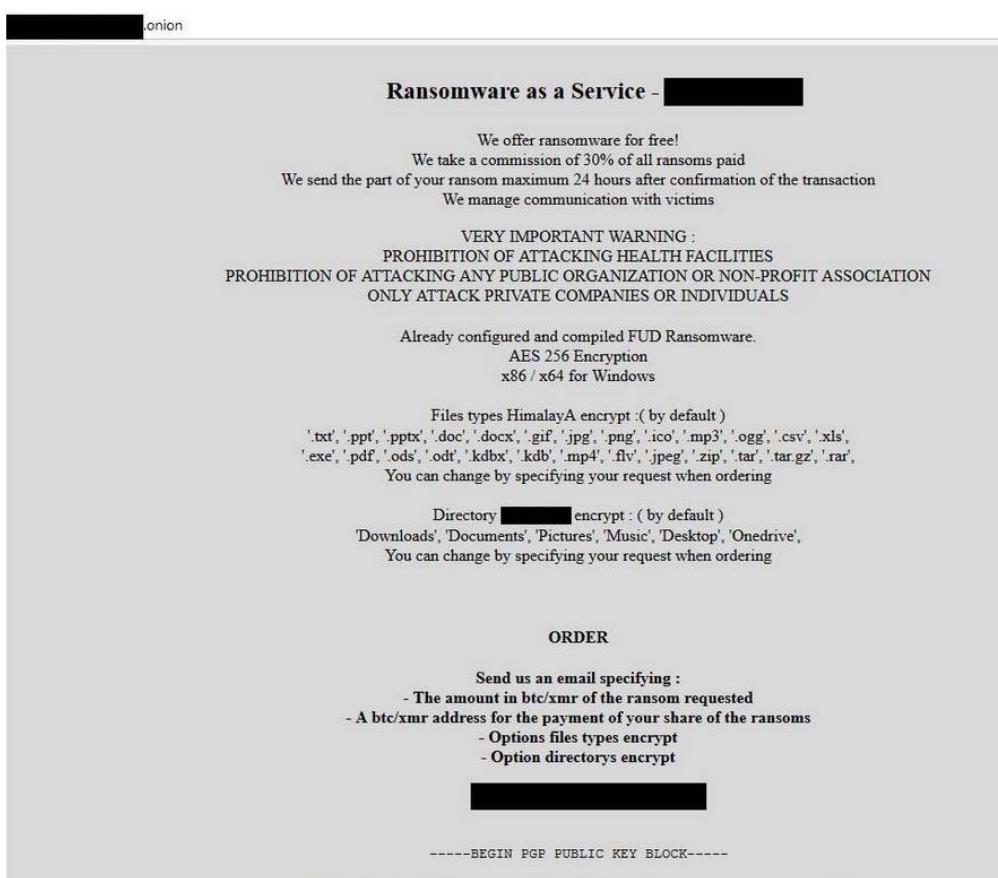
I will do anything for money, I'm not a pussy. If you want me to destroy some business or a persons life, I'll do it!
Some examples:
- Simply hacking something technically
- Creating a technical trouble on websites / networks to disrupt their service with DDOS and other methods.
- Espionage
- Getting private information from someone
- Ruining your opponents, business or private persons you don't like, I can ruin them financially and/or get them arrested, whatever you like.
If you want someone to get known as a child porn user, no problem.

The following prices are estimates, if I think a specific job takes more time and money I will either refund you or you will send the remaining once we talked.
If you are unsure about which category to choose, choose the lower priced one in question.
You will receive successful jobs, if I can not do anything for you I will refund you. But keep in mind depending on your target specific things might take longer and require an addition payment, but only after I can can show some success.

Product	Price	Quantity
Small Job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.03096 B	<input type="button" value="1 X"/> <input type="button" value="Buy now"/>
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.06191 B	<input type="button" value="1 X"/> <input type="button" value="Buy now"/>
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites	900 EUR = 0.11144 B	<input type="button" value="1 X"/> <input type="button" value="Buy now"/>
UPGRADE! INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If I need longer this will get refunded. Only buy this together with one of the other options.	200 EUR = 0.02477 B	<input type="button" value="1 X"/> <input type="button" value="Buy now"/>

\$2000 MILLIARDS DE REVENUS EN 2019¹.

Le Ransomware : un VRAI business !!



PRIX MOYENS DE VOS DONNÉES SUR LE DARK WEB

Cartes de crédit clonées et données associées

Produit	Prix moyen sur le dark web
Carte Mastercard clonée avec code PIN	15 \$
Clonage d'une carte American Express	35 \$
avec un code PIN	
Carte VISA clonée avec code PIN	25 \$
Détails de la carte de crédit, solde du 12 \$	
compte jusqu'à 1000 \$	
Détails de la carte de crédit, solde du 20 \$	
compte jusqu'à 5000 \$	
Les identifiants bancaires de compte en ligne volés, minimum 100 \$ sur le compte	35 \$
Identifiants bancaires de compte en ligne volés, minimum 2000 \$ sur le compte	65 \$
Compte Walmart avec une carte de crédit	10 \$

Documents falsifiés

Produit	Prix moyen sur le dark web
Permis de conduire américain, qualité moyenne	70 \$
Permis de conduire américain, haute qualité	550 \$
Carte d'assurance automobile	70 \$
Carte de membre du service routier d'urgence AAA	70 \$
Relevé bancaire de Wells Fargo	25 \$
Relevé bancaire de Wells Fargo avec des transactions de	80 \$
Carte d'étudiant de l'université Rutgers	70 \$
Passeport américain, canadien ou européen	1500 \$
Carte d'identité nationale européenne	550 \$

Les médias sociaux

Produit	Prix moyen sur le dark web
Compte Facebook piraté	74,5 \$
Compte Instagram piraté	55,45 \$
Compte Twitter piraté	49 \$
Compte Gmail piraté	155,73 \$
Followers sur Instagram x 1000	7 \$
Followers sur Spotify x 1000	3 \$
Followers sur Twitch x 1000	6 \$
Followers sur Tick Tok x 1000	15 \$
Followers sur LinkedIn x 1000	10 \$
Followers d'une page d'entreprise LinkedIn x 1000	10 \$
Followers sur Pinterest x 1000	5 \$
Nombre d'écoutes sur Soundcloud x 1000	1 \$
Vues sur Daily Motion x 1000	2 \$
Twitts et retweets x 1000	25 \$
likes sur Instagram x 1000	6 \$

Les attaques DDoS

Produit	Prix moyen sur le dark web
Site web non protégé, consultations par seconde, 1 heure	10 à 50 000 10 \$
Site web non protégé, demandes par seconde, 24 heures	10-50 000 60 \$
site web non protégé, demandes par seconde, 1 semaine	10 à 50 000 400 \$
Site web non protégé, demandes par seconde, 1 mois	10-50k 800 \$
Site web Premium protégé, requêtes par seconde, 24 heures	20 à 24 200 \$
50 000 requêtes par seconde, 24 heures	50 000 requêtes par seconde, 24 heures

LA CPME : PARTENAIRE FONDATEUR ET HISTORIQUE DE CYBERMALVEILLANCE.GOUV.FR



La CPME a été un des membres fondateurs du dispositif gouvernemental d'assistance aux cybervictimes, Cybermalveillance.gouv.fr qui a vu le jour en 2017, et y participe activement depuis lors

IMPLICATIONS DE LA CPME DANS LES ACTIONS DE CYBERMALVEILLANCE.GOUV.FR



La CPME est élue et représentée aux A.G. et au C.A de Cybermalveillance.gouv.fr dans le collège utilisateurs



A ce titre, elle participe aux travaux des Groupes de Travail de Cybermalveillance.gouv.fr sur les divers projets en cours de production tels que la qualification ou la création d'outils d'aide à la cybersécurité spécifiquement pour le TPE/PME.

Exemples:

- gestionnaire de mots de passe
- Auto Evaluation cyber permettant l'évaluation de l'entreprise en termes de cybersécurité, et les mesures à prendre pour diminuer le risque.
- Etc.



Assistance et prévention
en sécurité numérique

LE CYBERMOI/S EUROPÉEN DE LA CYBERSECURITÉ (CHAQUE ANNÉE EN OCTOBRE)

Les mots de passe ? Vous en avez probablement eu des dizaines, si ce n'est des centaines. Vous avez l'habitude d'en inventer, et vous connaissez déjà les recommandations habituelles : ne pas les réutiliser, varier majuscules et minuscules, utiliser des chiffres... Les mots de passe, ça vous connaît. Mais êtes-vous sûr que les vôtres soient vraiment inviolables ? Cet octobre, le Cybermoi/s vous donne toutes les clés pour mieux gérer et renforcer vos mots de passe !

COMMENT LA CPME S'IMPLIQUE T-ELLE DANS LE CYBERMOI/S ?

-  Participation au Groupe de Travail piloté par l'ANSSI à la définition du contenu national de la campagne et sa déclinaison sur le mois d'Octobre
-  Au niveau National : Un webinaire dédié organisé le 22 Octobre prochain à 9H (information sur le site de la CPME et sur les réseaux sociaux Twitter : [@CPMEnationale](#) ; Facebook : [CPME](#) ; LinkedIn : [CPME nationale](#))
-  Au niveau local : des CPME, des fédérations adhérentes organisent, coorganisent ou contribuent à des événements dédiés à la cyber en octobre (comme le CMCS !!)



Toutes les ressources sont sur :
<https://www.cybermois.fr/>



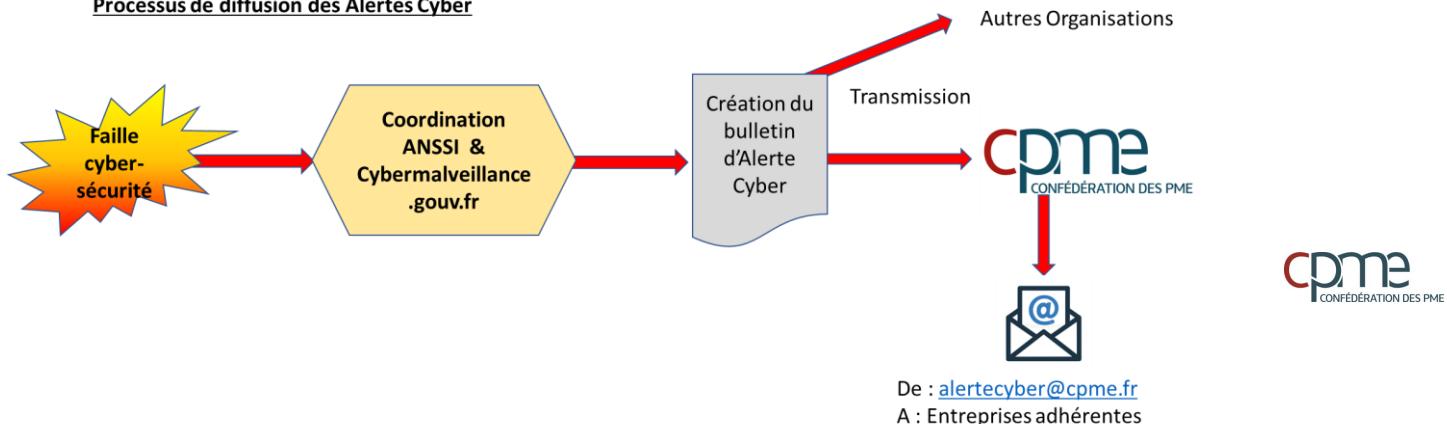
LA CPME PARTIE PRENANTE DE L'ALERTE CYBER DESTINÉE AUX DIRIGEANTS DE TPE-PME

Mardi 20 juillet, le secrétaire d'Etat au numérique Cédric O a annoncé le déploiement de l'Alerte Cyber, déployée notamment avec la CPME

DESCRIPTION DU MÉCANISME D'ALERTE

-  Le principe ? Lorsqu'un risque de sécurité du réseau informatique important se présente, l'Alerte Cyber sera diffusée par la CPME à ses adhérents via un mail dédié : alertecyber@cpme.fr pour qu'elle soit adressée aux chefs d'entreprise
-  Le déclenchement de l'alerte se fera à l'initiative de l'agence publique de la sécurité informatique française l'ANSSI et de Cybermalveillance.gouv.fr , la plate-forme gouvernementale d'assistance aux victimes de cyber attaques.
-  Ces alertes consisteront essentiellement en des appels à faire des mises à jour de logiciels, pour remédier à une vulnérabilité récemment découverte.

Processus de diffusion des Alertes Cyber



LA SENSIBILISATION DES UTILISATEURS : UN ENJEU MAJEUR POUR SE PROTEGER ET PROTEGER SON ENTREPRISE

Mise en place de la visio-conférence, travail à distance... : les risques cyber sont encore plus présents, notamment pour les TPE-PME. Pour vous aider à sécuriser vos équipements et sensibiliser vos équipes, la CPME a publié, en partenariat avec l'ANSSI, un guide pratique qui vous accompagne pas à pas

LE GUIDE DES BONNES PRATIQUES DE L'INFORMATIQUE



Deuxième version du guide , fruit de la collaboration entre la CPME et l'ANSSI



Actuellement en cours de révision, pour être à jour des nouvelles formes de cyberattaques

Un guide simple, pratico-pratique à mettre entre toutes les mains !!



A télécharger sur :

<https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/>

ou

<https://www.cpme.fr/publications/guides/guide-des-bonnes-pratiques-de-linformatique>

LA SENSIBILISATION DES UTILISATEURS : UN ENJEU MAJEUR POUR SE PROTEGER ET PROTEGER SON ENTREPRISE (SUITE)

Un guide pour mieux comprendre la sécurité numérique et protéger votre entreprise !

Ce guide vous donne les clés pour mieux comprendre la réalité du risque aujourd'hui et protéger votre entreprise. Il délivre des repères et conseils essentiels et apporte la vision des entreprises et experts de la cybersécurité.

L'ESSENTIEL DE LA SÉCURITÉ NUMÉRIQUE POUR LES DIRIGEANTS ET LES DIRIGEANTES



Deuxième version du guide largement enrichi et mis à jour, Le guide Sécurité numérique du CEIDIG- (Conseil de l'Économie et de l'Information du Digital) dont la CPME est partenaire



A télécharger sur :

https://www.nxtbook.fr/newpress/CEIDIG/l_essentiel-de-la-securite-numerique-pour-les-dirigeants-et-les-dirigeantes-2eme-edition/index.php?xtor=cigref#/p/C2

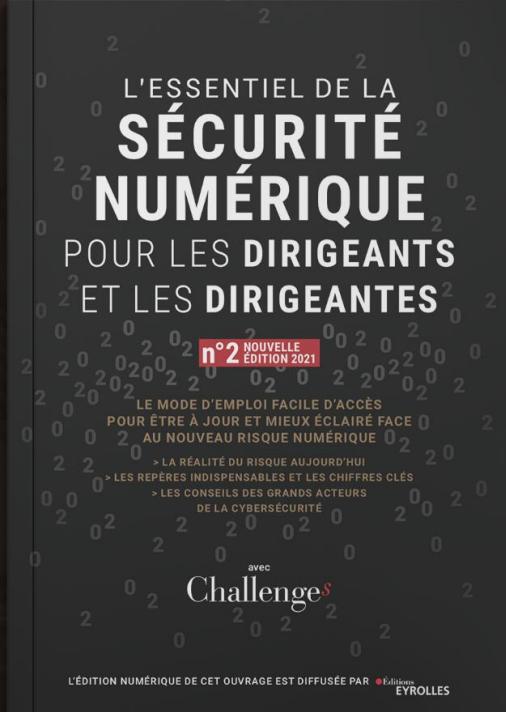
Merci de votre attention



Les conseils de protection cyber et leur mise en œuvre au sein de l'entreprise

Daniel Benabou,

Conseil de l'économie et
de l'information du digital
(CEIDIG), Co-président



"ENSEMBLE,
PROTÉGEONS NOTRE
ÉCONOMIE,
PROTÉGEONS NOS
ENTREPRISES"



Daniel Bénabou, président du CEIDIG
Conseil de l'économie et de l'information du digital



17

MEMBRES
COMITÉ
ÉDITORIAL



21

CONTRIBUTEUR
S



22

ORGANISATION
S PARTENAIRES



+200 H

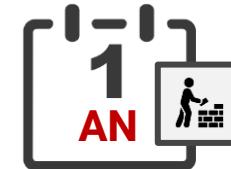
INTERVIEWS

+1 500
FICHIERS



25

MESSAGES VIDÉOS



Challenge's

Éditions
EYROLLES



+500 000

exemplaires numériques



16 000

exemplaires imprimés



1 150 inscrits

Contexte Éléments clés



1

ATTAQUES MASSIVES ET ULTRA SOPHISTIQUÉES : DU SUR-MESURE À GRANDE ÉCHELLE



Les Echos

« La cybercriminalité, principal risque pour l'économie », selon Jerome Powell



Les États-Unis vont accorder aux piratages par ransomware la même priorité qu'au terrorisme.
Département d'État à la Justice US



"L'absence de limites technologiques à ce que nous pouvons faire doit nous faire réfléchir à ce que nous devons faire" Barak Obama

1

La sécurité numérique doit rejoindre la maturité de la sécurité physique



2

► Maturité : 4 piliers du succès



RÈGLEMENTATION

Cadre : règles à respecter –
organisation
sanction - incentive



SENSIBILISATION

Pourquoi je dois agir



FORMATION

Comment je dois, je peux agir



OUTILS

Les moyens pour agir

3

La majorité des attaques peut être évitée



52 %

EXPLOITATION
D'UN DÉFAUT DE
CONFIGURATION
OU MAUVAIS
PARAMÉTRAGE ;
ABSENCE DE MOT DE
PASSE, DROIT ÉLEVÉ
SUR UN SERVEUR...)

60 %

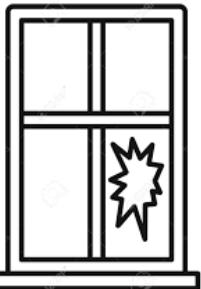
DES CYBERATTAQUES
PEUVENT ÊTRE
ATTRIBUÉES À DES
COMPORTEMENTS
HUMAINS
INADÉQUATS*,
PLUS ENGAGÉS,
MIEUX FORMÉS
LES SALARIÉS
SONT UN ELEMENT
DE DÉFENSE
IMPORTANT.

Bureau de la cybersécurité
des entreprises - Cnam
C - 2021

*Accenture, « State of
Cybersecurity Report 2020 »

Il existe des solutions **ACCESSIBLES** pour réduire considérablement l'impact d'un problème de cybersécurité





Victime préparée



Victime non-préparée

...aujourd'hui, vraiment victime ?

Actions possibles pour

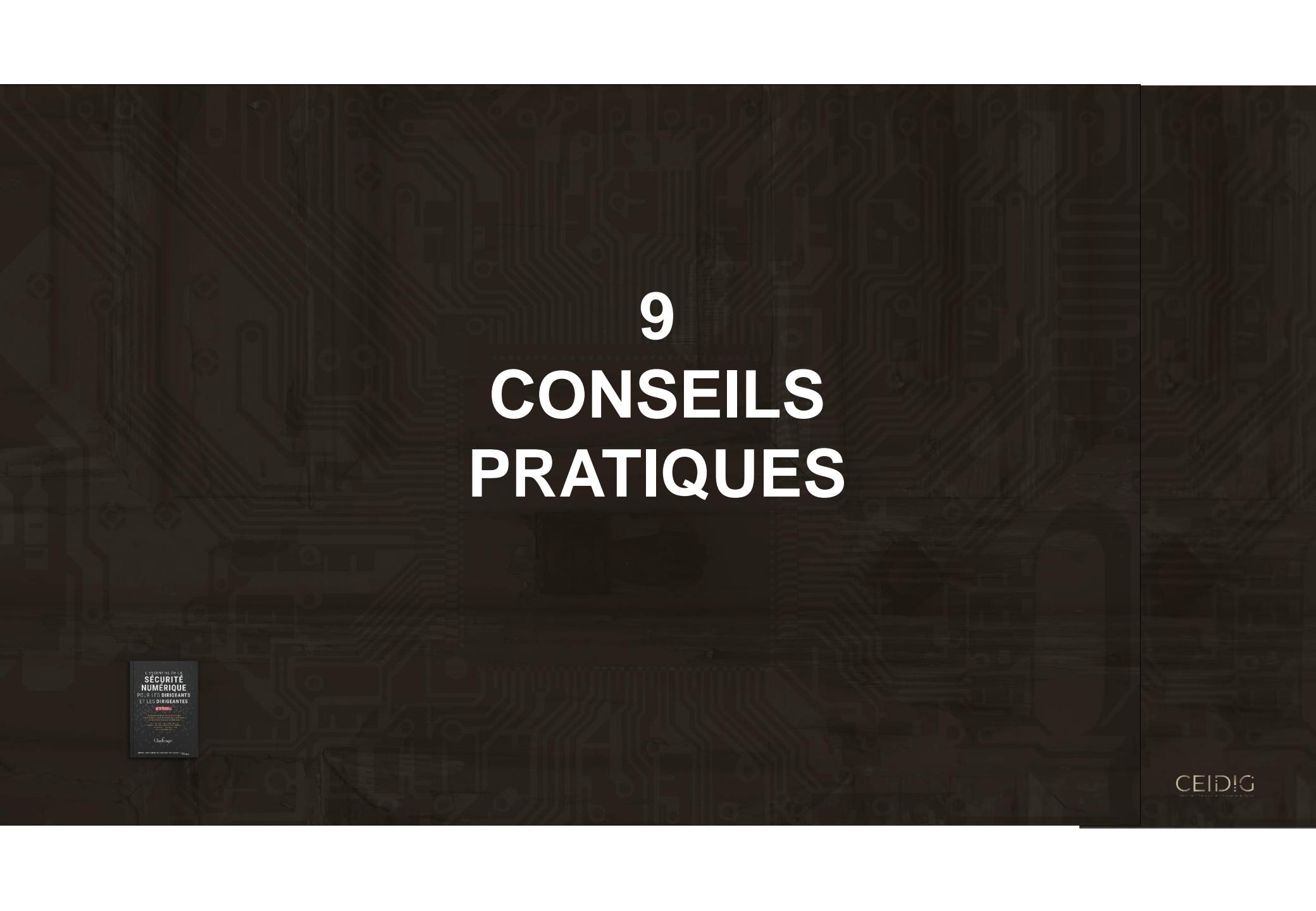
Limiter son exposition
Ne pas être une cible
facile



Ne pas laisser un incident faire
des dégâts considérables,
affecter la vie même de
l'entreprise

Dégâts conscrits / être capable de repartir
► résilience





9 CONSEILS PRATIQUES



CEIDIG
Centre d'expertise en cybersécurité

La sécurité numérique est un sujet transversal de l'entreprise

Security by design

La sécurité est envisagée dès la conception d'un projet, de tous les projets, la sécurité est abordée dans la vie de l'entreprise, son organisation, sa communication,....



Nommer un responsable



Sensibiliser, responsabiliser les salariés

FAITES VOUS ACCOMPAGNER



Avoir un dispositif adapté
Anticiper / être prêt pour pouvoir réagir très vite



Mettre en place un dispositif de sécurité performant et adapté exige un éventail de compétences et d'expertises difficilement disponibles dans l'entreprise. De même, en cas d'attaque, **l'aide d'un conseil expert** est souvent indispensable. Il peut permettre d'augmenter de façon déterminante la capacité et l'efficacité de la réaction. Identifier un partenaire pour accompagner son entreprise et ses collaborateurs en charge de la sécurité est donc aujourd'hui essentiel.

Limiter l'impact / Limiter l'exposition au risque

GESTION DES DROITS QUI DOIT POUVOIR FAIRE QUOI ?



L'attribution de droits élevés n'est ni un signe de confiance, ni une reconnaissance, ni un signe de position sociale, ...
Un manager responsable doit demander à ne pas avoir de droits d'administrateur s'il n'en a pas besoin



Limiter les droits à ce qui est strictement nécessaire est une règle de saine gestion

Les collaborateurs ne sont pas administrateurs de leurs PC, ni des applications de l'entreprise, sauf nécessité absolue



Si besoin d'avoir des droits élevés, avoir 2 comptes

Limiter l'impact / Retrouver son activité - Retrouver ses données
Prioriser

Identifier les activités et les données critiques, indispensables au fonctionnement de l'entreprise



Quel dispositif pour les protéger / les retrouver



Quelle organisation de substitution



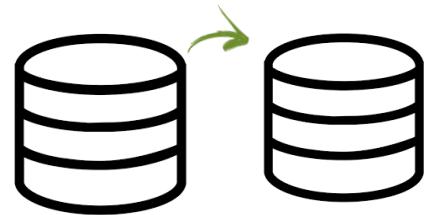
Faire un suivi régulier



Quid en cas de crise majeure ? Que feriez-vous ? Entraînez vous - posez vous la question

Limiter l'impact / Retrouver son activité - Retrouver ses données

SAUVEGARDER



Sauvegarde
indépendante !



Le plus régulièrement possible

Éviter l'impact

POSTES DE TRAVAIL ET SERVEURS À JOUR



Élimine les failles de sécurité sur
lesquelles s'appuient les attaquants



Immédiatement, dès la mise à jour disponible

Éviter l'impact

METTRE EN PLACE UN ANTI SPAM - ANTI PHISHING



Filtre de très nombreuses
attaques automatisées

Éviter l'impact

Mot de passe

PHRASE DE PASSE



Des mots de passe
différents !!!

Des solutions de gestion de mot
de passe



Double authentification pour
les accès, documents,
applications sensibles et
accessibles depuis internet



Changer le plus régulièrement possible



Faites votre algorithme

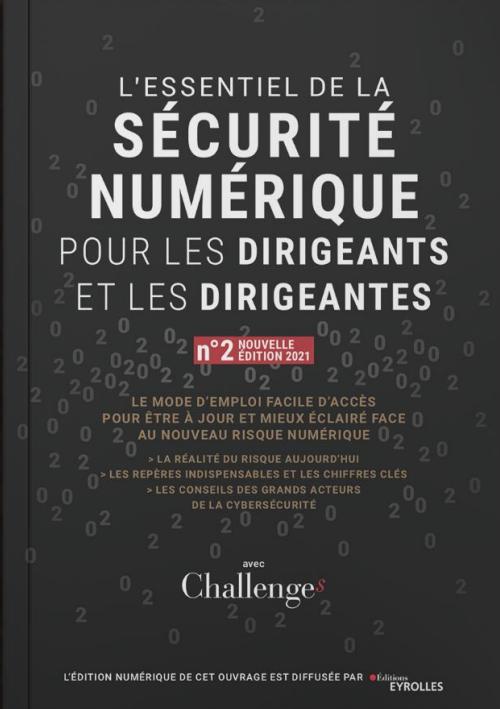
Règle N°

Réussir son dispositif de sécurité = renforcer son niveau de défense = éviter l'impact / limiter fortement l'impact

DONNER L'EXEMPLE



Bon sujet de leadership



Merci

ceidig.fr

CEIDIG
Centre d'Innovation et de Développement
des Industries Génierie et Numérique



Réponses aux interrogations

*Rédigez-les dans
l'onglet « questions »*

MERCI POUR VOTRE ATTENTION
ET VOTRE PARTICIPATION !

Pour toute information : contact@cpme.fr

LA CPME EST LA PREMIÈRE ORGANISATION INTERPROFESSIONNELLE
À ÊTRE CERTIFIÉE ENGAGEMENT DE SERVICE QUALI'OP

