21 octobre 2021

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

ENGAGEMENT DE SERVICE
QUALI'OP
REF. 166
AFNOR CERTIFICATION
www.afnor.org

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 »

cpme CONFÉDÉRATION DES PME

INTRODUCTION

La protection cyber, notion indissociable de celle de transition numérique

Alain Assouline

CPME,

Président de la Commission numérique

cpme CONFÉDÉRATION DES PME

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

Marc Bothorel

CPME,

Référent cybersécurité

cpme CONFÉDÉRATION DES PME

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

MMA Entrepreneurs d'Assurances

10To de données volées

orange Business Services

339Mo données
20 clients touchés

Rabot Dutilleul Construction

Rançon 8M Euros

facebook

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

In Extenso experts-comptables

Rançonné +15 jours sans accès dossiers client
Avril 2021

MPM MARSEILLE PROVENCE METROPOLE

3 mois de remise en état

Cadiou Industrie

« 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)

mom GROUP, GoGo squeeZ, Materne, Monts Blanc

Fermeture des serveurs
Arrêt des sites de production

in

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

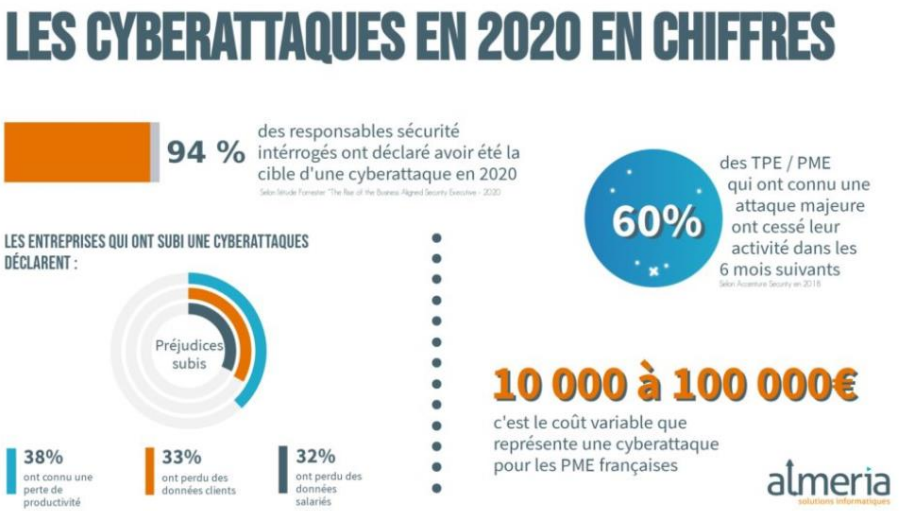
Vecteurs d'attaque :

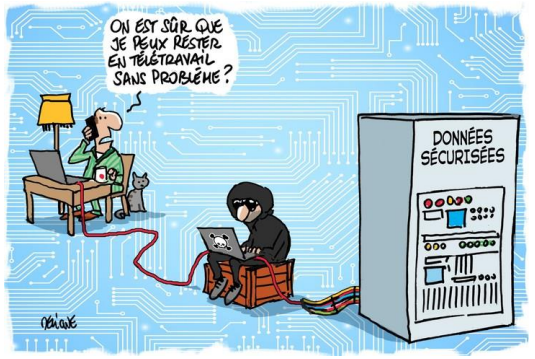
Grande sociétés ➔ ingénierie sociale, phishing
PME ➔ principalement les failles RDP/RDS, phishing

(1) Article du Télegramme du 15 Juillet 2020

cpme CONFÉDÉRATION DES PME

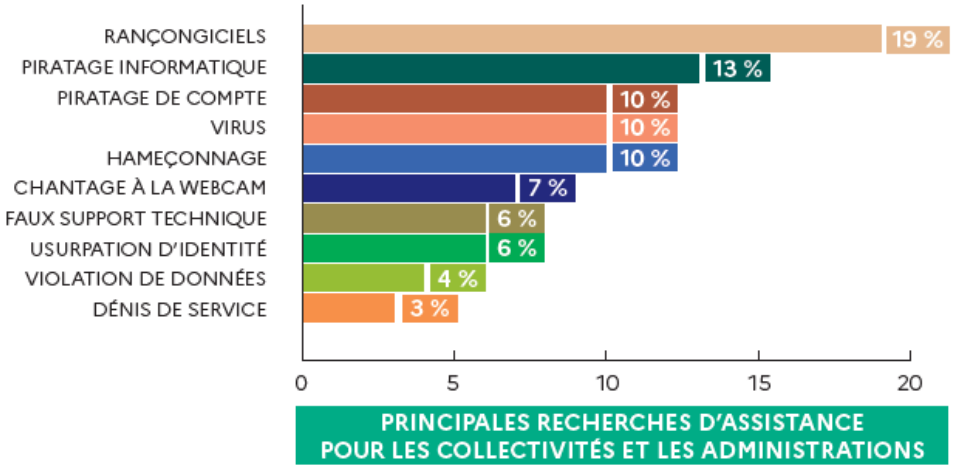
QUELQUES CHIFFRES SUR L'ACTIVITÉ CYBERCRIMINELLE EN 2020 (FRANCE)

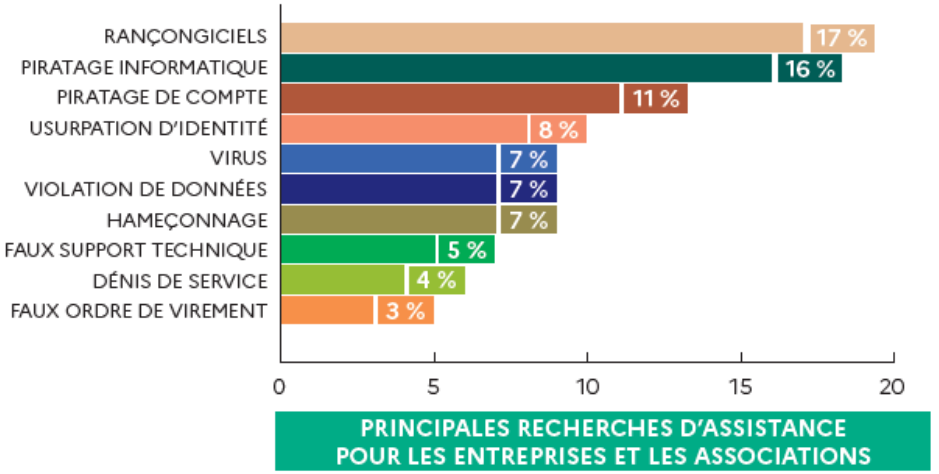




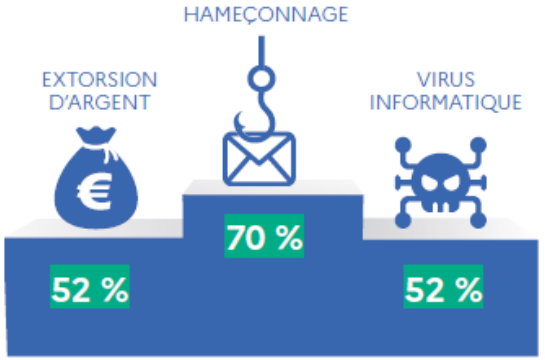
cpme CONFÉDÉRATION DES PME

QUELS SONT LES PRINCIPAUX ACTES DE CYBERMALVEILLANCE EN 2020 EN FRANCE[1]?





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



*Rapport cybermalveillance.gouv.fr 2020

cpme CONFÉDÉRATION DES PME

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 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

cpme CONFÉDÉRATION DES PME

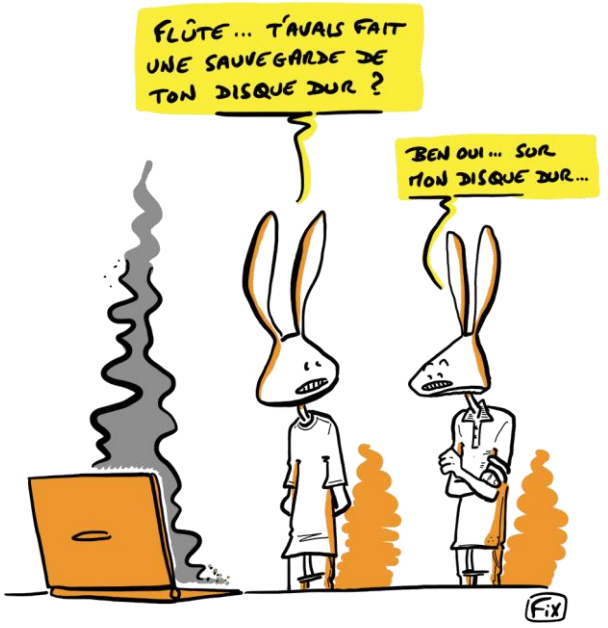
LES IMPACTS SUR NOS/VOS ENTREPRISES

Après annonce d'un cyber incident[1]:

- 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 robustes[2]
- **86%** des entreprises françaises n'ont pas souscrit à une cyberassurance[3]

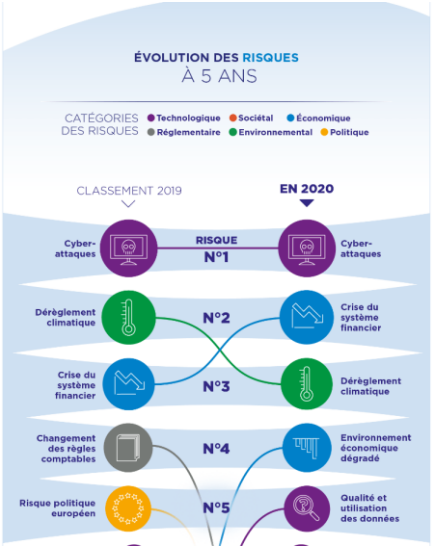


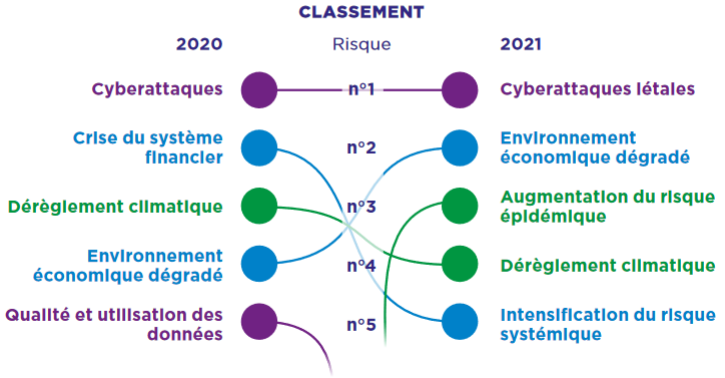
[1]: source Etude cabinet Bessé [2]: Source IBM Ponemon [3]: Source CLUSIF

cpme CONFÉDÉRATION DES PME

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://www.ffa-assurance.fr

cpme CONFÉDÉRATION DES PME

QUELQUES CARTES INTERACTIVES EN TEMPS RÉEL DES CYBERMENACES….

https://threatmap.checkpoint.com/

https://cybermap.kaspersky.com/stats

https://threatmap.bitdefender.com/

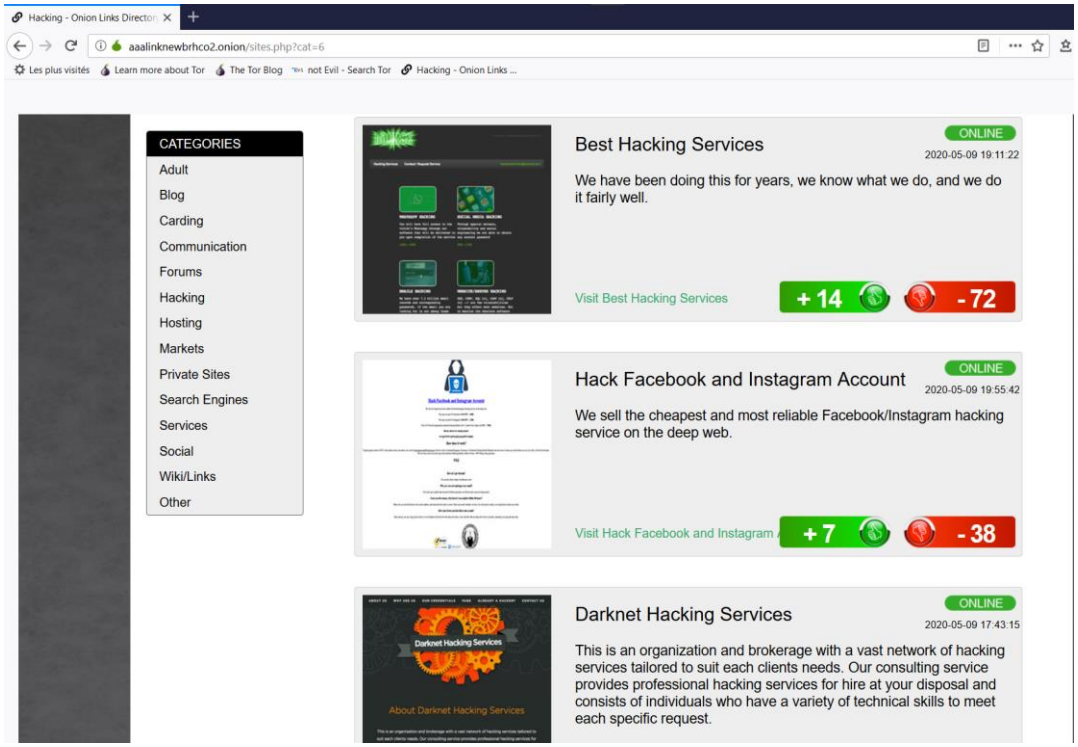
https://www.digitalattackmap.com/

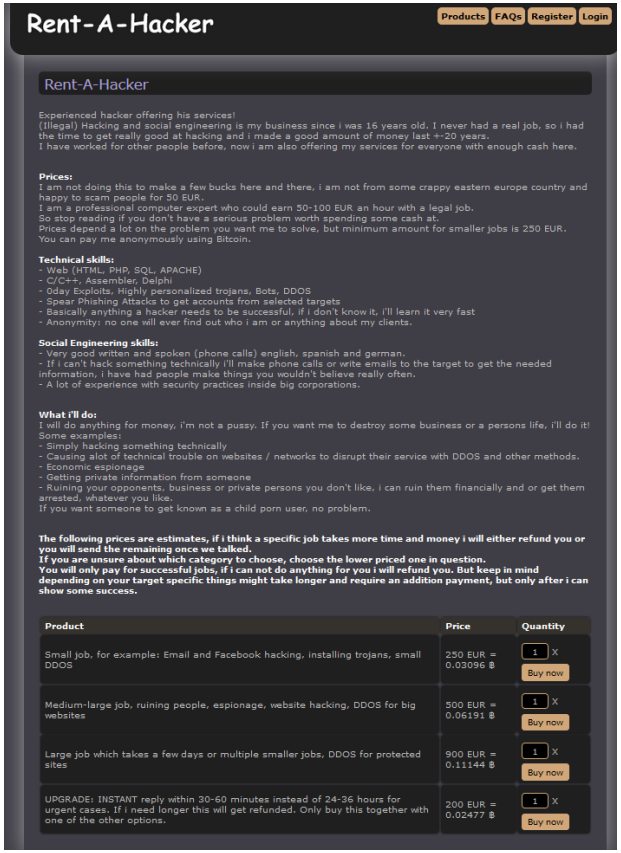
WEB – DEEPWEB - DARKWEB ???

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

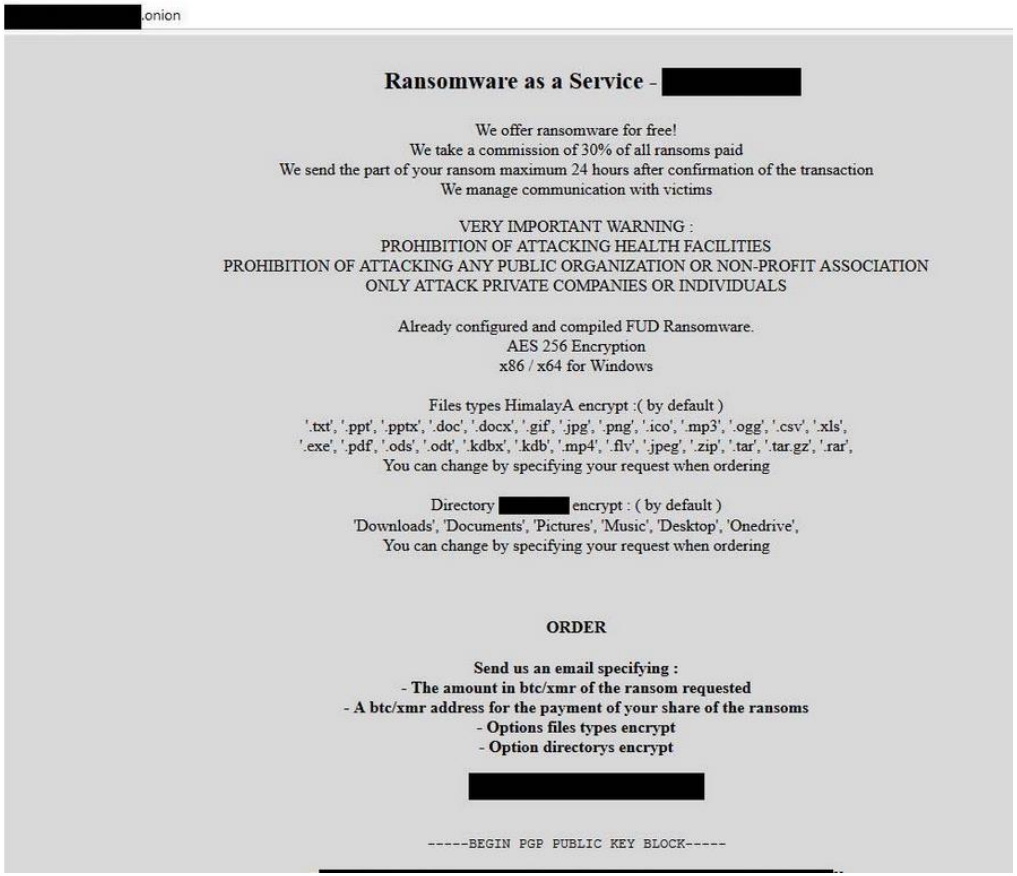




$2000 MILLIARDS DE REVENUS EN 2019[1].

cpme CONFÉDÉRATION DES PME

Le Ransomware : un VRAI business !!



[redacted].onion

Ransomware as a Service - [redacted]

We offer ransomware for free!
We take a commission of 30% of all ransoms paid
We send the part of your ransom maximum 24 hours after confirmation of the transaction
We manage communication with victims

VERY IMPORTANT WARNING :
PROHIBITION OF ATTACKING HEALTH FACILITIES
PROHIBITION OF ATTACKING ANY PUBLIC ORGANIZATION OR NON-PROFIT ASSOCIATION
ONLY ATTACK PRIVATE COMPANIES OR INDIVIDUALS

Already configured and compiled FUD Ransomware.
AES 256 Encryption
x86 / x64 for Windows

Files types HimalayA encrypt :(by default)
'.txt', '.ppt', '.pptx', '.doc', '.docx', '.gif', '.jpg', '.png', '.ico', '.mp3', '.ogg', '.csv', '.xls',
'.exe', '.pdf', '.ods', '.odt', '.kdbx', '.kdb', '.mp4', '.flv', '.jpeg', '.zip', '.tar', '.tar.gz', '.rar',
You can change by specifying your request when ordering

Directory [redacted] encrypt : (by default)
'Downloads', 'Documents', 'Pictures', 'Music', 'Desktop', 'Onedrive',
You can change by specifying your request when ordering

ORDER

Send us an email specifying :
- The amount in btc/xmr of the ransom requested
- A btc/xmr address for the payment of your share of the ransoms
- Options files types encrypt
- Option directorys encrypt

[redacted]

-----BEGIN PGP PUBLIC KEY BLOCK-----

[redacted]

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 dune carte American Express avec un code PIN	35 $
Carte VISA clonée avec code PIN	25 $
Détails de la carte de crédit, solde du compte jusqu'à 1000 $	12 $
Détails de la carte de crédit, solde du compte jusqu'à 5000 $	20 $
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 de 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, 10 à 50 000 consultations par seconde, 1 heure	10 $
Site web non protégé, 10-50 000 demandes par seconde, 24 heures	60 $
site web non protégé, 10 à 50 000 demandes par seconde, 1 semaine	400 $
Site web non protégé, 10-50k demandes par seconde, 1 mois	800 $
Site web Premium protégé , 20 à 50 000 requêtes par seconde, 24 heures	24 200 $

cpme CONFÉDÉRATION DES PME

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.

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 connait. 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 évènements dédiés à la cyber en octobre (comme le CMCS !!)

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

cpme CONFÉDÉRATION DES PME

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

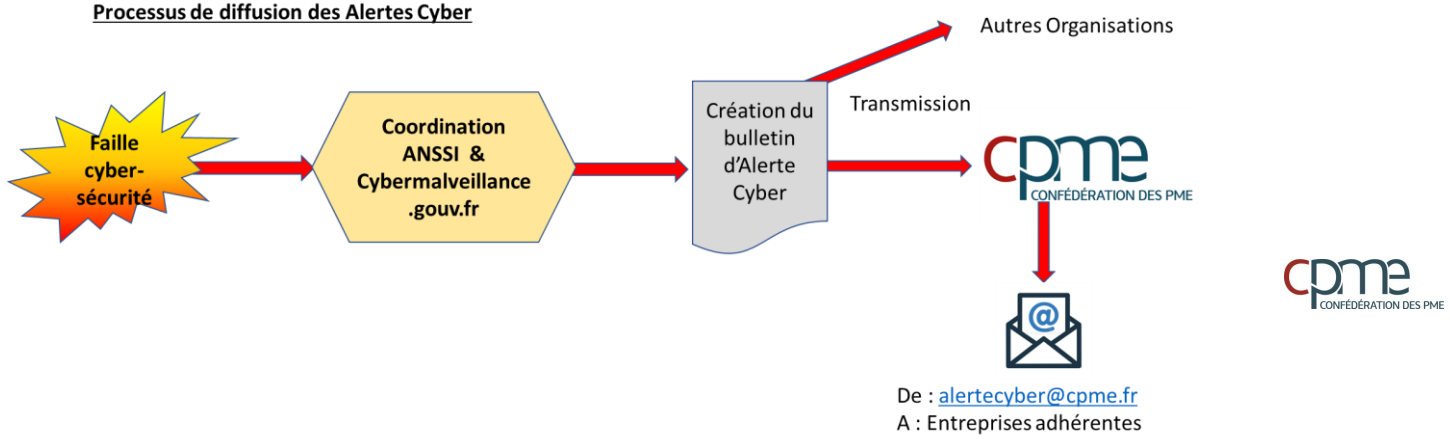
Mardi 20 juillet, le secrétaire d'Etat au numérique Cédric O a annoncé le déploiement de l'Alerte Cyber, déployée notamment avec la CPME

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 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.



cpme CONFÉDÉRATION DES PME

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

cpme CONFÉDÉRATION DES PME

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

cpme CONFÉDÉRATION DES PME

Merci de votre attention

cpme
CONFÉDÉRATION DES PME

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

cpme CONFÉDÉRATION DES PME

"ENSEMBLE, PROTÉGEONS NOTRE ÉCONOMIE, PROTÉGEONS NOS ENTREPRISES"

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

Ensemble, protégeons notre économie, protégeons nos entreprises

17 MEMBRES COMITÉ ÉDITORIAL

21 CONTRIBUTEURS

22 ORGANISATIONS PARTENAIRES

+200 H INTERVIEWS

+1 500 FICHIERS

25 MESSAGES VIDÉOS

1 AN

Challenges · Éditions EYROLLES · CESIN · AMRAE · Cigref · CYBER · GITSIS · SN · LES ASSISES · devoteam · EGERIE · GATEWATCHER · IDECSI · LINK BYNET · Orange Cyberdefense · MEDEF · cpme · Croissance plus · FRANCE DIGITALE · meti · FRANCE DIGITALE

+500 000

exemplaires numériques

1 150 inscrits

16 000

exemplaires imprimés

CEIDIG

Contexte
Éléments clés

CEIDIG

1

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

Les Echos

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

CNBC

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

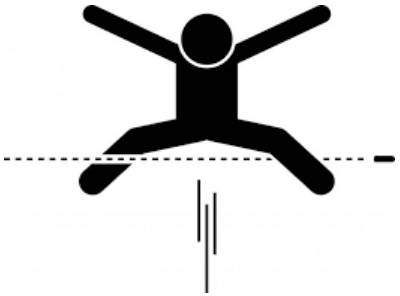
Comment je dois, je peux agir

OUTILS

Les moyens pour agir

3

La majorité des attaques peut être évitée



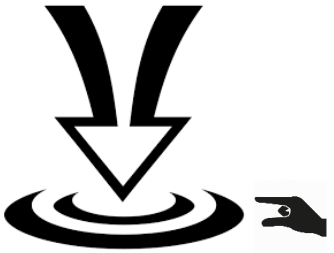
52%
EXPLOITATION D'UN DÉFAUT DE CONFIGURATION (MAUVAIS PARAMÉTRAGE : ABSENCE DE MOT DE PASSE, DROIT ÉLEVÉ SUR UN SERVEUR...)

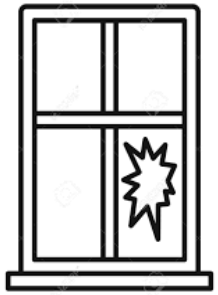
Baromètre de la cybersécurité des entreprises, Cesin

60%
DES CYBERATTAQUES PEUVENT ÊTRE ATTRIBUÉES À DES COMPORTEMENTS HUMAINS INADÉQUATS*. PLUS ENGAGÉS, MIEUX FORMÉS, LES SALARIÉS SONT UN LEVIER DE DÉFENSE IMPORTANT.

*Accenture, « State of Cybersecurity Report 2020 »

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





très

≠

Victime préparée

Victime non-préparée

...aujourdhui, 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

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 pouvoir réagir très vite

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

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

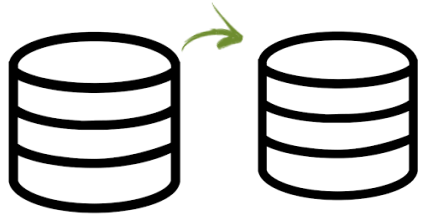
Quelle organisation de substitution

Faire un suivi régulier

Quid en cas de crise majeure ? Que feriez-vous ? Entrainez 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

EN OCTOBRE J'AGIS POUR LE CYBER MOIS

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

CONFÉDÉRATION DES PME

Réponses aux interrogations

Rédigez-les dans l'onglet « questions »

CONFÉDÉRATION DES PME

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

ENGAGEMENT DE SERVICE
QUALI'OP
REF. 166
AFNOR CERTIFICATION
www.afnor.org