Risques Cyber et de Fraude :

Ça n'arrive pas qu'aux autres!
Comment y faire face ?

URIOPSS Occitanie et BANQUE POPULAIRE DU SUD, avec la participation de Gras-Savoye

Mercredi 1er décembre 2021

BANQUE POPULAIRE DU SUD

GRAS SAVOYE
Willis Towers Watson

Le contexte des risques Cyber et Fraude

Risques Cyber, Risques de Fraude

La presse en parle….

« *Entre 2019 et 2020, en France, le nombre d'attaques a augmenté de 255%. Menace informatique la plus sérieuse pour les entreprises et les institutions, par le nombre d'attaques quotidiennes et leur impact sur la continuité d'activité, les rançongiciels visent particulièrement, depuis 2020, les secteurs de la santé et de l'éducation, les collectivités territoriales ainsi que les prestataires de services numériques*. »

Novembre 2021 par l'ANSSI et le BSI

« Fraude au président : la crise sanitaire a déclenché une nouvelle vague d'attaques »
latribune.fr, 26 Jan 2021,

« Cyberattaques en France : « La menace croit, plus grand monde n'est à l'abri »

Ouest France, 11 juin 2021

« *La menace cyber n'a jamais autant pesé sur les organisations, il y a désormais urgence à agir pour minimiser les surfaces d'attaque, identifier et limiter leurs effets afin d'assurer la continuité de service*. »

Les Echos, 16 novembre 2021

« Ils se font passer pour le président de l'entreprise et l'arnaquent de 15 millions d'euros »
Capital.fr, 19 février 2021

« Attaques par rançongiciel : les collectivités de plus en plus ciblées »

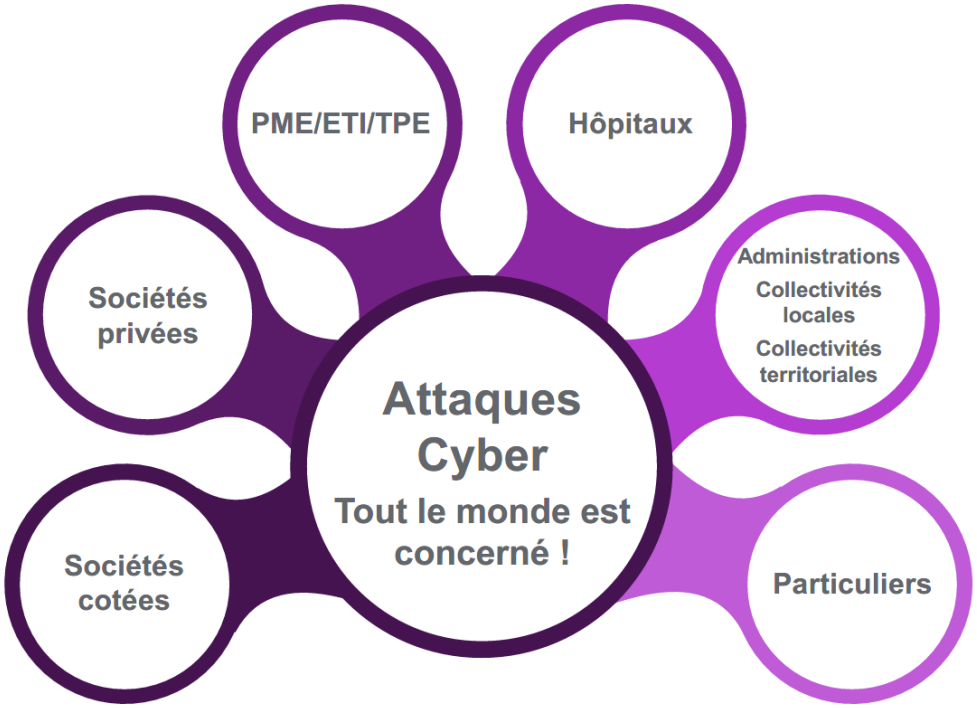
Zepros Territorial, 28 novembre 2021

« Toutes les entreprises sont aujourd'hui concernées, des artisans aux grands groupes en passant par les PME et les professions libérales. En 2020, plus d'une entreprise sur deux aurait été victime d'une cyberattaque, selon le Club des Experts de la Sécurité de l'Information et du Numérique. La menace est donc bien réelle. »

Nice-Matin, 26 novembre 2021

Risques Cyber

Une exposition mondiale qui affecte tout type d'organisation et qui est une réalité en France



Etc…

Risques Cyber

Le ransomware : la grande inquiétude des entreprises

La menace que représente le rançonlogiciel n'est pas nouvelle. Or, la rentabilité des attaques *ransomware*, le contexte de télétravail, ainsi que la prolifération et la professionnalisation des groupes d'hackers, notamment dû à l'apparition du Ransomware As A Service (RaaS), ont abouti à une **augmentation drastique du nombre d'attaques** durant l'année 2020. Ces dernières sont de plus en plus **évoluées**, **fréquentes** et leurs dégâts se chiffrent en **millions**.

192 incidents en 2020

+255%

54 incidents en 2019

300 millions €

Extorqués via Ransomware en 2020

18% **La proportion d'entreprise française ayant versé une rançon**

Tant en France que dans le monde, aucun secteur d'activité ou taille d'entreprise n'est épargné. Toute entreprise possédant un accès internet peut être infectée par un ransomware. Cependant, certaines entreprises ou institutions sont plus touchées par les attaques de ce type, dû notamment à la nature de leurs activités :

Secteur de la santé (hôpitaux)

Collectivités locales (mairies)

Secteur de l'éducation (universités)

Entreprises du secteur privé, particulièrement des services numériques (ESN)

Chiffres français 2020 basés sur le rapport de l'ANSSI : « ÉTAT DE LA MENACE RANÇONGICIEL À L'ENCONTRE DES ENTREPRISES ET INSTITUTIONS »

Qu'entend-on par risques Cyber ?

Définition : les conséquences d'une atteinte aux données numériques détenues et/ou gérées par l'entreprise, que celles-ci lui appartiennent ou qu'elles lui soient confiées par des tiers, ainsi que les conséquences d'une atteinte au système informatique.

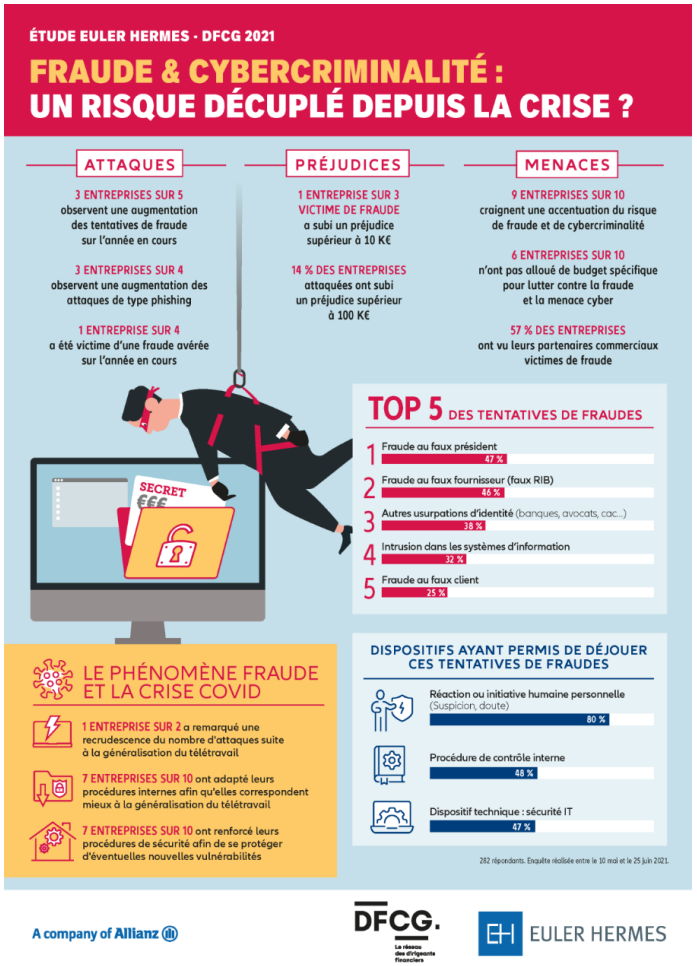
Les atteintes aux données numériques

- **Vos données** nécessaires à l'activité,
- **Les données appartenant aux Tiers**,
- Les données de vos collaborateurs,
- Les données des clients,
- Les données des fournisseurs, sociétés partenaires…
- **L'atteinte à la réputation** : diffamation, atteinte à la protection de la vie privée, atteinte aux droits à l'image, atteinte aux droits de propriété intellectuelle d'un tiers

Les atteintes au système informatique

- **Intrusion** dans les systèmes informatiques,
- **Interruption** des systèmes informatiques.
- **Contamination** des systèmes (virus, bombe logique…)
- **Utilisation illégale** des systèmes et du réseau.
- **L'atteinte à la réputation** : pertes de chiffre d'affaires, atteinte à l'image de la société…

Risques de Fraude



Quels enseignements ?

- 2 entreprises sur 3 ont subi au moins une tentative de fraude cette année, et 1 entreprise sur 5 a subi plus de 5 attaques ;
- 33% des entreprises victimes de fraude ont subi un préjudice supérieur à 10K €, et 14% ont subi un préjudice supérieur à 100K € ;
- Effet Covid-19 : près d'une entreprise sur deux a remarqué une recrudescence des attaques suite à la généralisation du télétravail
- Des attaques récurrentes, pour une efficacité croissante des fraudeurs
- Des attaques récurrentes, pour une efficacité croissante des fraudeurs
- L'usurpation d'identité plébiscitée, mais très complémentaire des outils cyber

Source : Baromètre Fraude et Cybercriminalité 2021, Euler Hermes / DFCG

Qu'entend-on par risque de Fraude ?

Les Fraudes externes : l'usurpation d'identité

- Fraudes au faux président
- Fraudes aux faux fournisseurs
- Autres usurpations d'identité
- Fraudes aux faux clients

Mais aussi….Les Fraudes internes

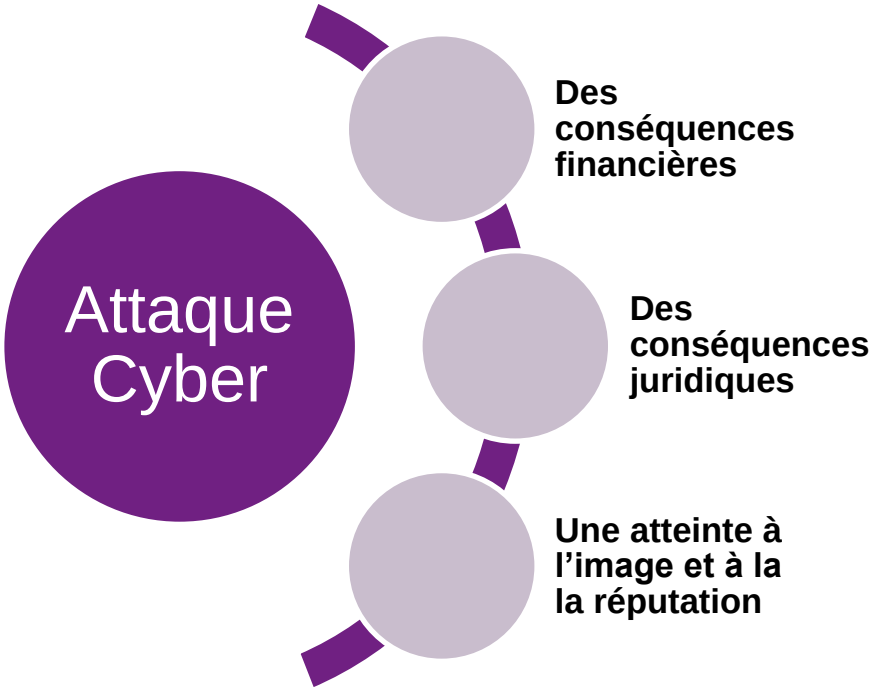
- Fraude interne : détournement de fonds, de marchandise, fausses factures.
- Le collaborateur-fraudeur est une personne qui bénéficie de la confiance du management : il est difficile à identifier.
- Durée moyenne des fraudes internes : > 18 mois (jusqu'à +10 ans).

Les conséquences d’une attaque Cyber et d’une Fraude

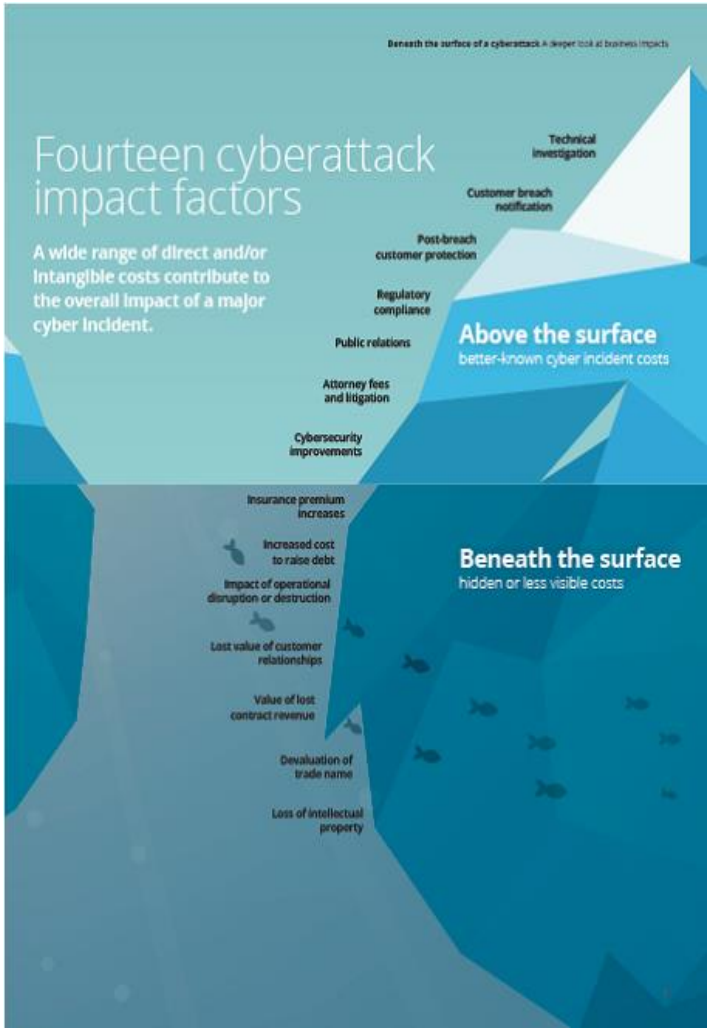
Attaques Cyber : Quelles conséquences ?

- Une Cyber-attaque peut générer une crise majeure pouvant remettre en cause la pérennité même de l'entreprise

- Les principales conséquences d'une cyber-attaque :



Attaques Cyber : Un risque aux conséquences multiples



1. Forensics (expertise informatique)
2. Frais de notification aux clients, consommateurs
3. Frais de monitoring et de surveillance
4. Frais d'enquête/défense et sanctions des autorités de protection des données (CNIL, ICO…)
5. Frais de communication /Relations Publiques
6. Honoraires d'avocat et Conséquences vis-à-vis des tiers (RC)
7. Améliorations de la Sécurité Informatique
8. Augmentation des primes d'assurance
9. Augmentation des coûts de financement (taux d'intérêt)
10. Impacts sur l'activité : interruption ou arrêt d'activité
11. Impact relation clients/prospects
12. Perte de clients et de contrats
13. Réduction de la valeur de la marque
14. Perte de droits de Propriété Intellectuelle

Source : Etude Deloitte, 2016 "Beneath the surface of a cyberattack : A deeper look at business impacts"

Attaques Cyber : Typologie des risques et des dommages

Atteinte aux données personnelles

Risques RC et Dommage (avec ou sans réclamation de tiers)

- Frais de notification
- Frais de consultants (Forensics)
- Frais en cas d'enquête d'une autorité de contrôle
- Frais de Défense
- Sanctions Pécuniaires

Atteinte aux systèmes d'information ou aux données appartenant à l'assuré

- Vol, ajout, soustraction, détérioration, destruction
- Impossibilité d'utilisation des systèmes (Déni de service) / arrêt des systèmes
- Atteinte à l'image / gestion de crise / défaçage
- Contamination des systèmes et des données (attaque logique, virus…)
- Pertes d'Exploitation et les frais supplémentaires consécutifs

Atteinte aux données des tiers

Risque RC (dans le cadre d'une réclamation de tiers)

- Vol et destruction des données
- Interruption des services en ligne et réclamations de tiers
- Corruption des données, ajout, transformation, cryptage, détérioration, altération
- Erreur
- Frais de Défense et Conséquences Pécuniaires

La répartition des coûts d'un sinistre ransomware

Type de coûts (€)	Moyenne	Maximum
Perte d'exploitation	3 321 077	16 946 260
Paiement de la rançon	1 379 113	9 678 903
Heures supplémentaires	504 895	3 403 644
Coût de restauration / remédiation	1 013 137	8 664 261
Remplacement d'équipements	140 292	583 320
Frais d'experts informatique (forensics)	410 012	4 901 537
Expert en cyber sécurité	224 012	832 847
Frais juridique (hors frais de défense)	382 011	1 812 559
Frais de relation publique	265 877	1 828 050
Frais pour restaurer les données qui ont été perdues ou détruites	190 680	1 515682
Frais de coordinateur d'incident / gestion de crise	53 766	372 713

Source : Willis Towers Watson

Attaques Cyber

Implication croissante et rôle des Directions Générales face aux risques Cyber

WTW Directors' Liability Report "D&O: A new era of risk exposure", 2019/2020

Les risques Cyber sont un sujet majeur de gouvernance, compte tenu que :

- Les DG sont désormais très soucieuses de la protection des données en raison de la multiplication des incidents (vécus ou non) depuis quelques années

- Les risques Cyber sont des risques d'intensité qui pèsent sur tout type de de société, quelles que soient leur taille, leurs implantations, ou leurs activités

Exposition des Directions Générales face aux risques Cyber

- **Des enjeux de responsabilité personnelle:**
  - Les dirigeants sont responsables de la sécurité logique (protection des systèmes d'information et des données)
  - Des actions qui peuvent émaner des actionnaires / dirigeants / employés

- **Certaines affaires ont donné lieu à des actions en justice aux Etats-Unis**
  - Derivative action (action émanant des actionnaires)
    - *FTC v. Wyndham Worldwide Corp.* : les manquements de la société en matière de mesures de sécurité ont été considérés comme des **pratiques commerciales déloyales** au sens du FTC Act.
  - Actions de la SEC
    - *RT Jones* : l'absence de mise en place d'une politique de sauvegarde des informations de ses clients, a été considérée par la SEC comme une **violation délibérée d'une règlementation boursière**

- **Fondement : le défaut de supervision**
  - Ne pas avoir appréhendé les risques Cyber à la hauteur de leur enjeux au sein de la société
    - Nécessité d'impulser la réflexion en interne (en liaison avec les RSSI, les comités des risques et d'audit)
    - Etre capable d'arbitrer les choix stratégiques à faire en ce domaine (prioriser les actions de prévention, là où les enjeux sont vitaux pour l'entreprise)
  - Demain : risque de mise en cause pour ne pas avoir mis en place de contrat d'assurance ou souscription d'une limite de garantie insuffisante ?

Les conséquences d'une Fraude

Conséquences directes :		
Perte immédiate correspondant au montant du détournement de biens et/ou de valeurs	Perte, destruction, détérioration de données informatiques (actes de malveillances)	Perte d'exploitation consécutives

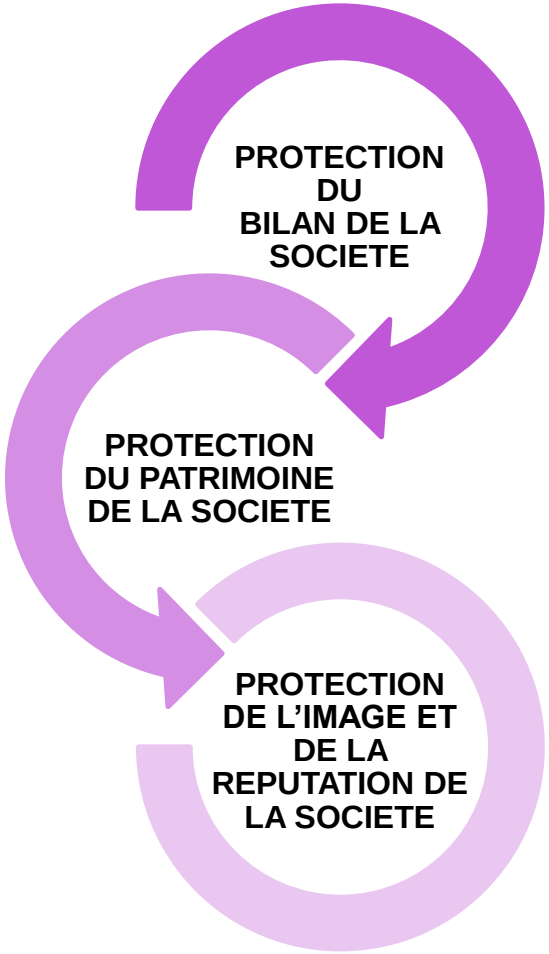
Conséquences indirectes :		
Perte d'image, de confiance, de réputation, de part de marché.	Baisse du cours de la bourse	Mise en cause personnelles des dirigeants.

L’assurance des risques Cyber et de Fraude

Contenu et intérêt

Objectifs des polices d'assurance Cyber

Gestion de la crise et transfert des conséquences financières



Contenu des polices d'assurance Cyber

- **Ce sont des polices combinées offrant** :
  - Des couverture Dommages,
  - Des couvertures Responsabilité Civile,
  - Un volet assistance.

55 % des entreprises françaises ne savent pas qu'il existe des produits de cyber-assurance visant à fournir une couverture et des services aux entreprises qui subissent une atteinte à la sécurité des données.
Source : Etude Lloyd's « Facing the cyber risk Challenge »,

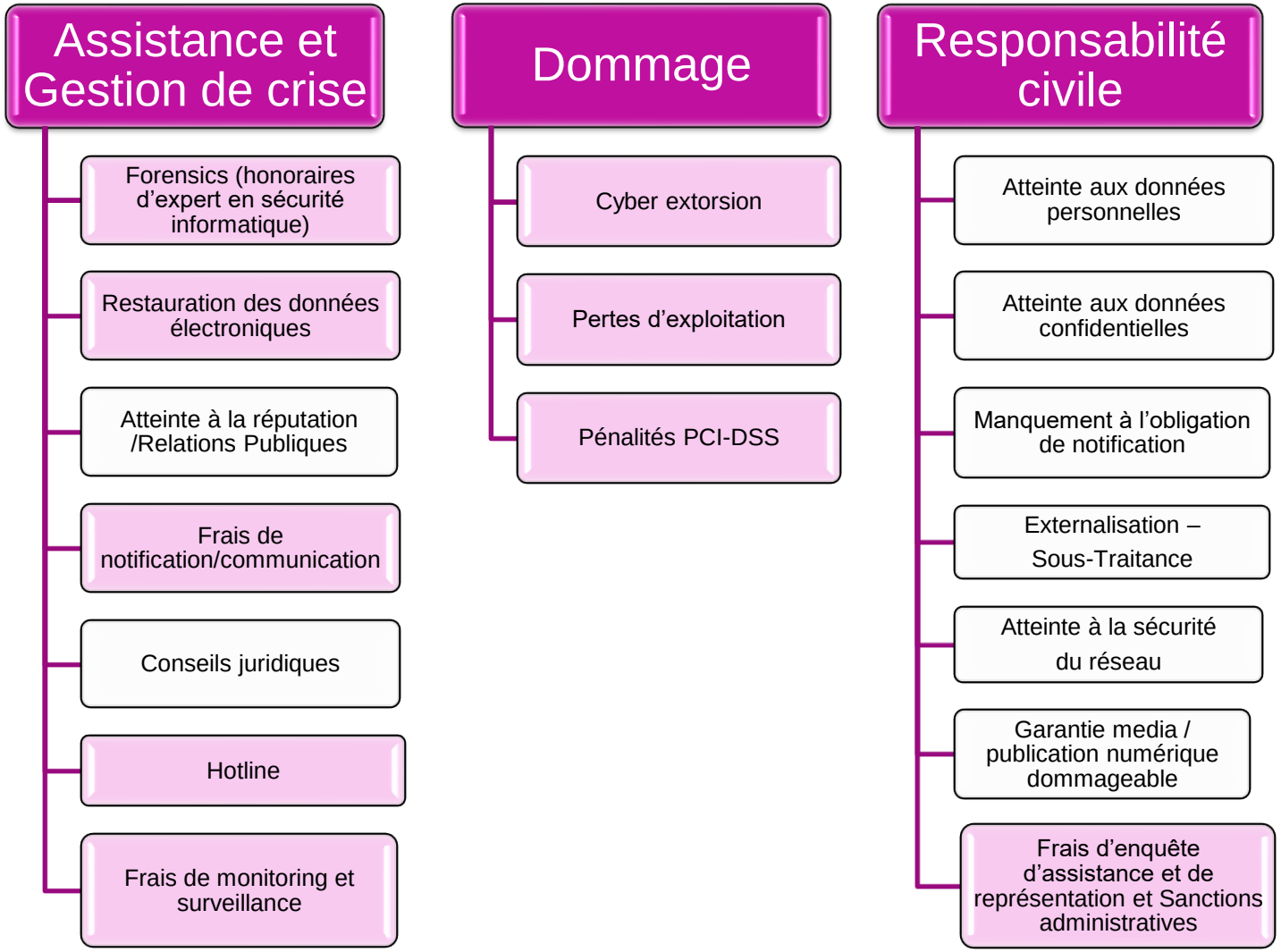
- **Ce sont des polices dédiées aux Cyber Risques**, apportant une réponse unique et complète à cette menace croissante avec le support de consultants/experts associés à l'assureur.

- **Ces contrats ont comme principaux avantages** :
  - Prise en compte simple et rapide des garanties d'assurance en cas de cyber-attaques,
  - Réactivité dans la gestion des sinistres (ex. : notification dans les délais impartis en cas de piratage des données personnelles).

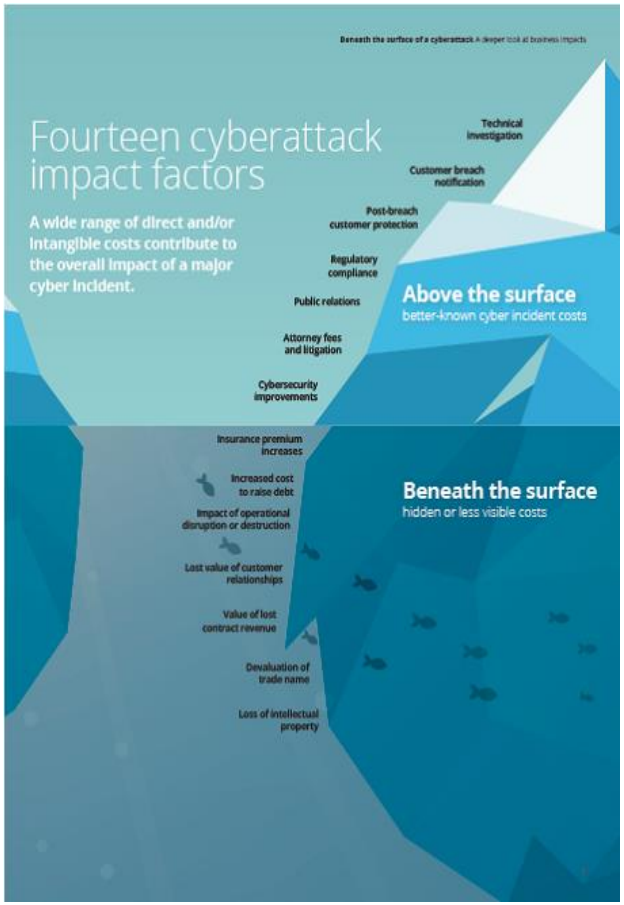
- **Ils peuvent intervenir en complément des garanties existantes dans les programmes d'assurances « traditionnels ».**

**Il est important de noter que les garanties proposées au titre des polices Dommages et/ou Responsabilités Civile, sont généralement sous-limitées ou partiellement couvertes.
Enfin, des exclusions spécifiques peuvent restreindre le champ d'application des contrats.**

Police d'assurance Cyber : Présentation des principales garanties



Police d'assurance Cyber : Quelle réponse aux conséquences d'une attaque Cyber ?



1. Forensics (expertise Informatique)
2. Frais de notification aux clients, consommateurs
3. Frais de monitoring et de surveillance
4. Frais d'enquête/défense et sanctions des autorités de protection des données (CNIL, ICO…)
5. Frais de communication /Relations Publiques
6. Honoraires d'avocat et Conséquences vis-à-vis des tiers (RC)

7. Améliorations de la Sécurité Informatique

8. Augmentation des primes d'assurance
9. Augmentation des coûts de financement (taux d'intérêt)
10. Impacts sur l'activité : interruption ou arrêt d'activité

11. Impact relation clients/prospects
12. Perte de clients et de contrats
13. Réduction de la valeur de la marque
14. Perte de droits de Propriété Intellectuelle

Coûts, Frais, Honoraires, Frais supplémentaires Pertes d'Exploitation et Conséquences Pécuniaires

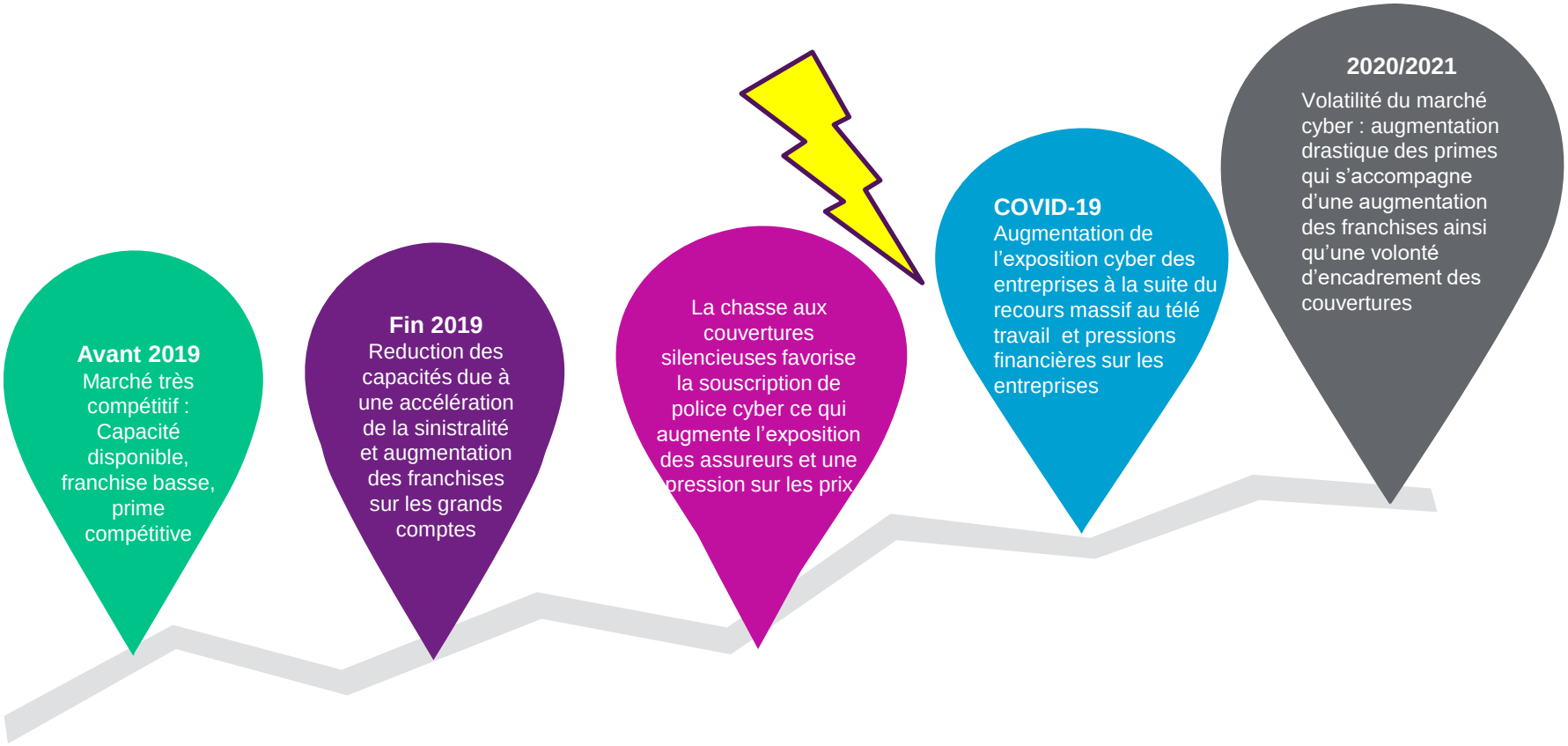
Couverts par un contrat Cyber risques

Police d'assurance Fraude : Présentation des principales garanties

Assuré	L'entreprise et ses filiales
Modalités d'application de la garantie	Sont couverts les fraudes ou les actes de malveillance découverts pendant la période de validité du contrat. Le sinistre est imputable à la période d'assurance au cours de laquelle la fraude ou l'acte de malveillance informatique est découvert. La limite de garantie est accordée par année d'assurance.
Prise en charge par l'assureur	▫ Des pertes pécuniaires directes subies par l'assuré résultant d'un acte frauduleux ▫ Des pertes pécuniaires indirectes ▫ Des frais d'expertise ▫ Des dépenses consécutives encourues par l'assuré au titre des frais de reconstitution d'Information, des frais supplémentaires d'exploitation et des frais de procédure

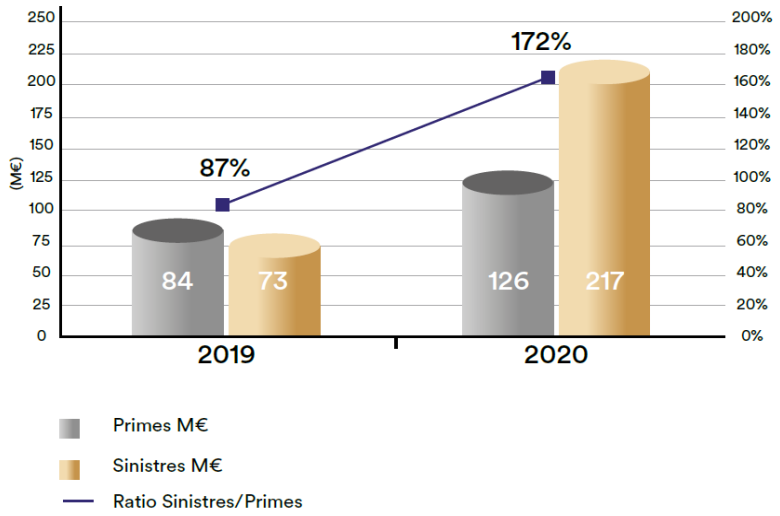
Le marché de l’assurance

L’évolution du marché de l’assurance Cyber



L'évolution du marché de l'assurance Cyber

Un marché très déséquilibré



87 % des grandes entreprises mais seulement **8 %** des entreprises de taille intermédiaire ont **souscrit une assurance cyber.**

38 M€ hauteur moyenne de la **couverture des grandes entreprises.**

X 3 : **augmentation de la sinistralité surtout en intensité :** le montant global des indemnisations a été multiplié par 3, passant de 73 M€ en 2019 à 216 M€ en 2020.

+ 19 % pour les grandes entreprises et **+ 28 %** pour les ETI : **augmentation des taux de primes entre 2019 et 2020.**

167 % vs 84 % **ratio Sinistres/Primes** de 2020 vs celui de 2019.

Source : Rapport LUCY, AMRAE

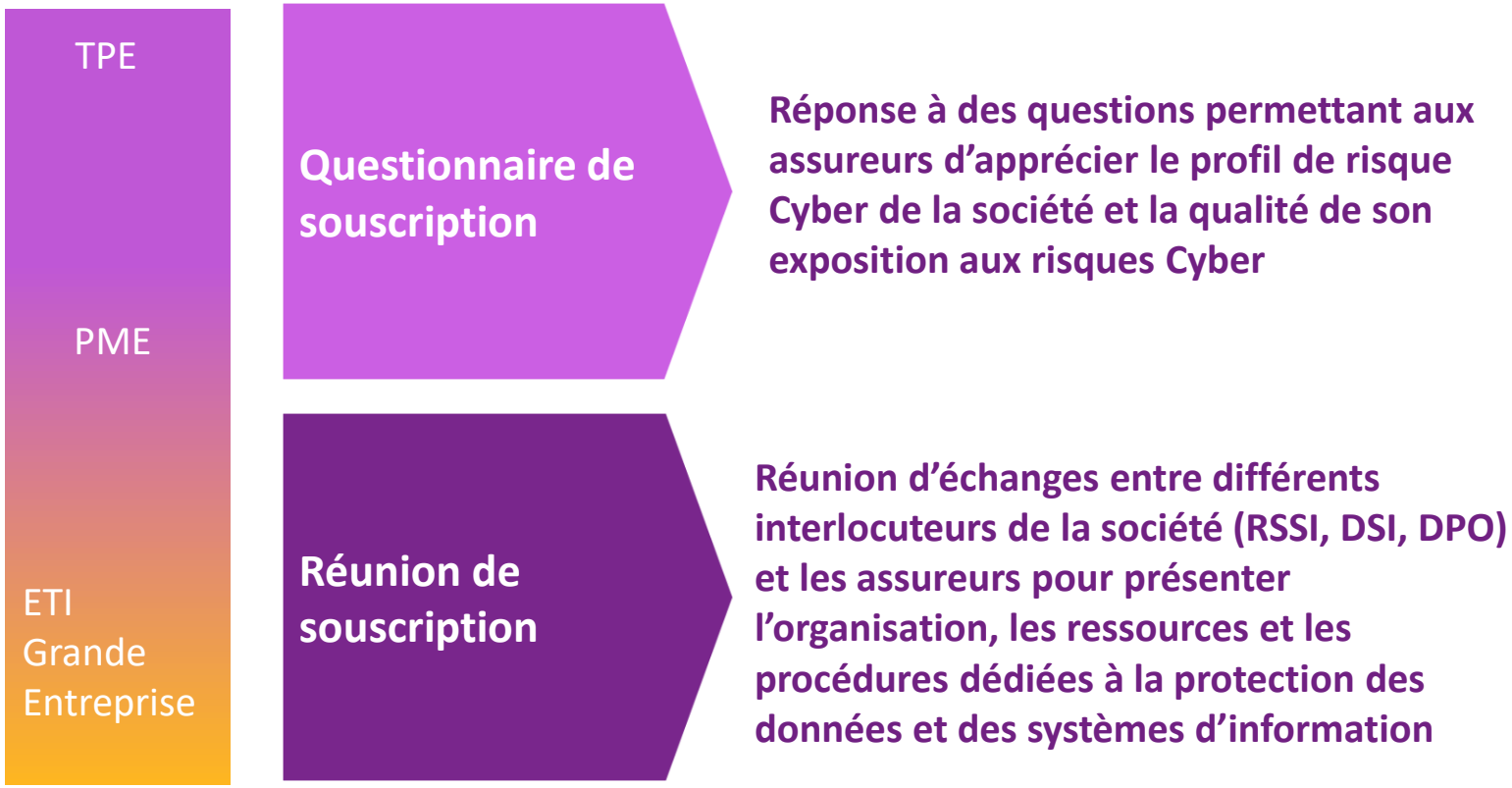
L'évolution du marché de l'assurance Cyber

Tendances du marché de l'assurance Cyber en 2021

Capacité et Souscription	Texte de police / Garantie	Sinistralité	Prime et Franchise
▪ Durcissement du marché depuis octobre 2020 ▪ Poursuite de la réduction des capacités tant en 1ère ligne qu'en Excess (maximum 10M€ en première ligne / 10M€ voire 15M€ en excess) ▪ Refus de positionnement en 1ère lignes pour certains assureurs, avec des points d'attachement excess variant de 50M€ à 100M€ ▪ Révision des interdictions/cibles de souscription au niveau mondial ▪ Questionnaires ransomware spécifiques imposés par les assureurs ▪ Réalisation à distance d'audits de vulnérabilité des SI des clients exposés sur Internet, dont les résultats déterminent leur souscription.	• Révision des sous limites accordées sur l'ensemble des portefeuilles. • Recadrage des textes sur les garanties de base (sous limitation des conséquences à la suite d'un évènement ransomware, sous limitation de la panne, non couverture de la panne chez le prestataire d'externalisation)	▪ Une sinistralité qui s'est intensifiée en fréquence et en intensité ▪ Loss ratio des assureurs fortement dégradé ▪ Le ransomware est devenu la première menace des entreprises et des assureurs ▪ Selon Ponemon Institute, le coût moyen d'une attaque par ransomware est de 4,4m$ ▪ Au-delà d'une augmentation des demandes de rançon, ce coût intègre également la perte d'exploitation et la restauration des systèmes.	▪ Redressement tarifaire particulièrement violent, avec des primes fortement augmentées (de 100% à 150% en moyenne, minimum 50% pouvant atteindre plus de 1000% pour les clients sinistrés). ▪ Introduction de clauses de coassurance de l'assuré (sur toutes les garanties liées à une attaque par ransomware, ou sur la garantie Perte d'Exploitation). ▪ Augmentation des franchises selon la taille et l'exposition des sociétés ▪ Les assurés ayant subi en 2020 des attaques Cyber ont été les plus impactés par ces hausses de franchise.

Méthodologie de souscription

Le questionnaire ou la réunion de souscription



Le questionnaire spécifique au risque de ransomware devient un impératif pour une grande majorité d'assureurs.

Conditions préalables au succès d'un placement / renouvellement d'une police cyber

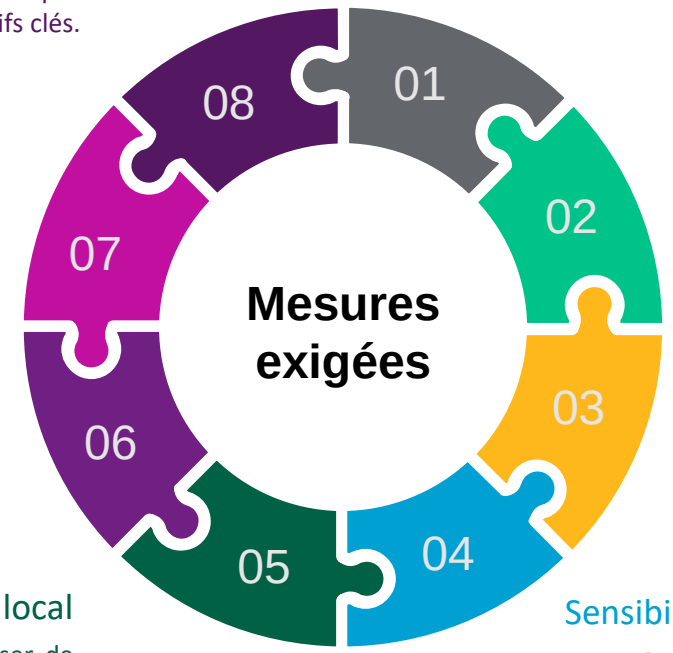
Les mesures exigées ("Need to have" measures)

Outil de gestion des accès privilégiés (PAM)

Un outil de gestion des accès privilégiés permettant de surveiller les comptes ayant un accès privilégié aux actifs clés.

Endpoint Detection & Response (EDR)

Mis en place sur tous les serveurs lorsque cela est possible



Authentication multi-facteur (MFA)

Mis en place et requis pour tous les accès distants au réseau de l'entreprise ainsi que pour toutes les connexions à Office365.

Gestion d'actifs informatiques

Inventaire de l'environnement à l'aide d'un outil de gestion des actifs.

Procédures de sauvegarde

Sauvegarde hors ligne ou solution de sauvegarde alternative rendant impossible la suppression des sauvegardes existantes

Centre d'Opération de Sécurité (SOC)

Surveillance du réseau.

Privilèges d'administrateur local

Les administrateurs locaux doivent disposer de comptes distincts pour leur utilisation quotidienne et pour les tâches nécessitant un accès administrateur..

Sensibilisation des employés

Des formations et/ou des campagnes de sensibilisation sont prévues et obligatoires pour tous les utilisateurs de technologies informatiques, au moins sur une base annuelle.

Conditions préalables au succès d'un placement / renouvellement d'une police cyber

Les mesures recommandées ("Good to have" measures)

Sécurité des e-mails

- Pré-scan des liens et des pièces jointes envoyés par courrier électronique.
- Méthode pour garantir que le courrier électronique entrant provient d'un expéditeur légitime (SPF, DKIM, DMARC).

Reprise après sinistre et réponse aux incidents

- Tests réguliers de récupération des sauvegardes
- Plan de réponse aux incidents formel et documenté

Sécurité réseau

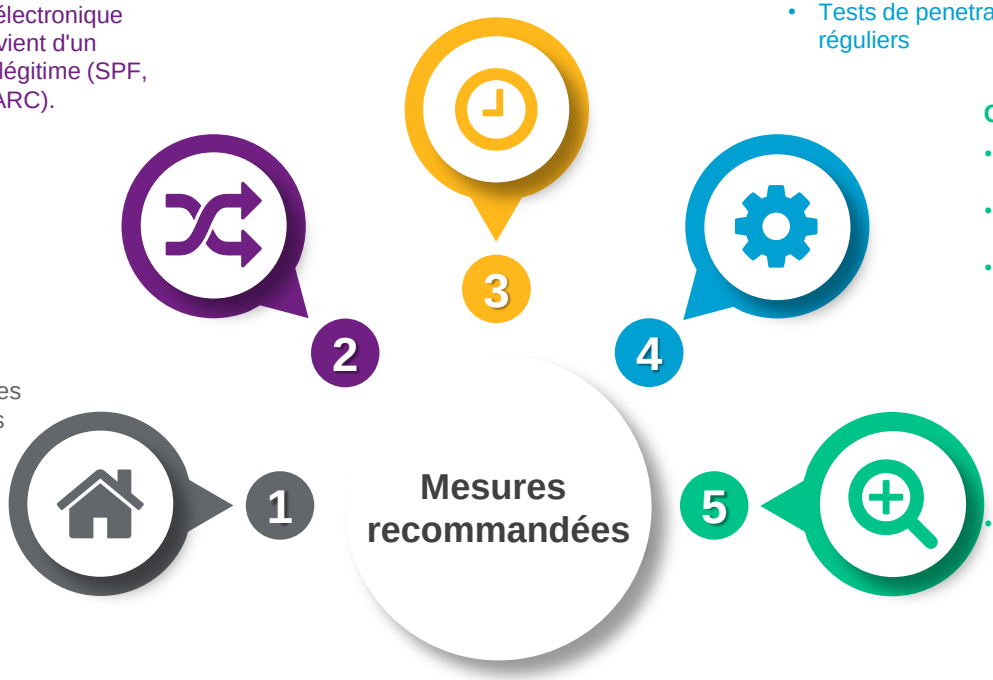
- Cryptage des sauvegardes
- Corrections automatisées
- Segmentation du reseau
- Tests de penetration réguliers

Capacités de détection

- Scans réguliers des vulnérabilités
- Outil d'examen des logs (SIEM)
- Les sources de logs doivent inclure au moins les pare-feu, de préférence également les AD, EDR et d'autres ressources critiques. EDR implémenté sur tous les clients du réseau
- NDR mis en place lorsque l'EDR n'est pas envisageable

Gestion des actifs

- Accès restreint aux services à partir des appareils personnels
- Solution de gestion des des appareils mobiles (MDM)



Et sans oublier l'importance des bonnes pratiques…

- Sensibiliser vos collaborateurs **et cadres aux risques,**
- Diffuser des procédures claires **aux collaborateurs mandatés sur les règles d'authentification des émetteurs et de confirmation des demandes de virement** imprévues ou de validation des changements de coordonnées bancaires
- **Déployer des solutions adaptées telles que l'authentification forte, la double validation pour les paiements, …**
- **Veiller à limiter la publication d'informations (site Internet, réseaux sociaux…) permettant d'identifier et de contacter vos collaborateurs habilités**
- **Généraliser l'utilisation de mots de passe solides pour les comptes de messagerie et activez la double authentification**
- **Appliquer de manière régulière et systématique les mises à jour de sécurité y compris sur les équipements mobiles**
- Faire des sauvegardes régulières

CONTACTS :

Marielle GIRERD :

marielle.girerd@groupebps.fr / 06.84.53.30.75

Hélène LANSAC:

helene.lansac@groupebps.fr

06.99.06.80.34

Merci pour votre attention !
Vous avez la parole !

GRAS SAVOYE, société de courtage d'assurance et de réassurance
Siège Social : Immeuble Quai 33, 33/34 quai de Dion-Bouton, CS 70001, 92814 Puteaux Cedex.
Tél : 01 41 43 50 00. Télécopie : 01 41 43 55 55. http://www.grassavoye.com.
Société par actions simplifiée au capital de 1 432 600 euros. 311 248 637 RCS Nanterre. N° FR 61311248637.
Intermédiaire immatriculé à l'ORIAS sous le n° 07 001 707 (http://www.orias.fr).
Gras Savoye est soumis au contrôle de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution) 61 rue Taitbout 75436 Paris Cedex 9