SecNumeco
ANSSI

SÉCURITÉ ÉCONOMIQUE & RISQUES CYBER

27 octobre 2022 / Limoges

ÉTAT DE LA MENACE, BONNES PRATIQUES & RETOURS D'EXPÉRIENCES

#SecNumEco

Organisé par :

ALIPTIC

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Liberté Égalité Fraternité
Direction générale des Entreprises

Avec le soutien de :

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE
Liberté Égalité Fraternité

RÉGION Nouvelle-Aquitaine

Limoges Métropole
Communauté urbaine

En collaboration avec :

MINISTÈRE DE L'INTÉRIEUR
Liberté Égalité Fraternité

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE
Nouvelle-Aquitaine

CLUSIR #Aquitaine

Université de Limoges

ADI Nouvelle-Aquitaine
Agence de Développement et d'Innovation

CCI LIMOGES HAUTE-VIENNE

E.S.T.E.R
LIMOGES TECHNOPOLE

DIGITAL AQUITAINE

En partenariat avec :

les acteurs de la compétence
Nouvelle-Aquitaine

ALLISNA
Alliances Innovation Santé Nouvelle-Aquitaine

ALPHA RLH

avrul
Agence pour la valorisation de la recherche universitaire du Limousin

cpme 87
HAUTE-VIENNE

CRYPTIS

FIBOIS NOUVELLE AQUITAINE

Gendarmerie nationale
Une force humaine

LIMOGES BUSINESS +++CLUB
LA FORCE D'UN RÉSEAU

Mouvement des Entreprises de France Limousin

PÔLE EUROPÉEN DE LA CÉRAMIQUE

POLICE NATIONALE

UIMM
LA FABRIQUE DE L'AVENIR

xlim

SecNumeco
ANSSI

Ouverture du SecNumEco

Mme Fabienne Balussou, Préfète de la Haute-Vienne
M. François Vincent, Conseiller régional Nouvelle-Aquitaine
M. Gilles Toulza, Vice-Président de Limoges Métropole

Organisé par :

ALIPTIC

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Liberté Égalité Fraternité
Direction générale des Entreprises

Avec le soutien de :

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE
Liberté Égalité Fraternité

RÉGION Nouvelle-Aquitaine

Limoges Métropole
Communauté urbaine

En collaboration avec :

MINISTÈRE DE L'INTÉRIEUR
Liberté Égalité Fraternité

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE Nouvelle-Aquitaine

CLUSIR #Aquitaine

Université de Limoges

ADI Nouvelle-Aquitaine
Agence de Développement et d'Innovation

CCI LIMOGES HAUTE-VIENNE

E.S.T.E.R
LIMOGES TECHNOPOLE

DIGITAL AQUITAINE

En partenariat avec :

les acteurs de la compétence Nouvelle-Aquitaine

ALLISNA Alliance Innovation Santé Nouvelle-Aquitaine

ALPHA RLH

avrul
AGENCE POUR LA VALORISATION DE LA RECHERCHE UNIVERSITAIRE DU LIMOUSIN

cpme 87 HAUTE-VIENNE

CRYPTIS
FORMATIONS EN CRYPTOLOGIE ET SÉCURITÉ DE L'INFORMATION

FIBOIS NOUVELLE AQUITAINE
UNIS POUR UNE FILIÈRE D'AVENIR

Gendarmerie nationale
Une force humaine

LIMOGES BUSINESS +++CLUB
LA FORCE D'UN RÉSEAU

Mouvement des Entreprises de France Limousin

PÔLE EUROPÉEN DE LA CÉRAMIQUE

POLICE NATIONALE

UIMM
LA FABRIQUE DE L'AVENIR

xlim

SecNumeco
ANSSI

Conférence

RISQUES CYBER ET IMPACTS SUR LA SANTÉ DES ENTREPRISES

Stéphane Mortier, Adjoint au Centre Sécurité Économique et Protection des Entreprises, Direction Générale de la Gendarmerie Nationale

Organisé par :

ALIPTIC

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Direction générale des Entreprises

Avec le soutien de :

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE

Région Nouvelle-Aquitaine

Limoges Métropole Communauté urbaine

En collaboration avec :

MINISTÈRE DE L'INTÉRIEUR

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE Nouvelle-Aquitaine

CLUSIR #Aquitaine

Université de Limoges

ADI Nouvelle-Aquitaine

CCI LIMOGES HAUTE-VIENNE

E.S.T.E.R Limoges Technopole

DIGITAL AQUITAINE

En partenariat avec :

les acteurs de la compétence Nouvelle-Aquitaine

ALLISNA

ALPHA RLH

avrul

cpme 87 Haute-Vienne

CRYPTIS

FIBOIS Nouvelle Aquitaine

Gendarmerie nationale

LIMOGES BUSINESS +++CLUB

Mouvement des Entreprises de France Limousin

Pôle européen de la céramique

POLICE NATIONALE

UIMM La fabrique de l'avenir

xlim

SecNumeco
ANSSI

Table ronde

ETAT DE LA MENACE

Alexia Dudognon, Commissaire de police, directrice adjointe DTPJ Limoges
Gilles Etienne, Spécialiste Cyber Police Nationale
Julien Gluchowski, Référent Intelligence Économique Gendarmerie Nationale
Martin Veron, Délégué à la Sécurité Numérique Nouvelle-Aquitaine ANSSI

Organisé par :

Avec le soutien de :

En collaboration avec :

En partenariat avec :

L'ÉTAT DE LA MENACE

L’ÉTAT DE LA MENACE

I. Auteurs de cyberattaques et motivations

Définition

Une cyber-attaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant.

Elle cible différents dispositifs informatiques connectés :

-des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet ;

-des équipements périphériques tels que les imprimantes ;

-ou encore des appareils communicants comme les téléphones mobiles, les smartphones ou les tablettes.

Les auteurs de cyberattaques

Ils peuvent être de toute sorte :

- des concurrents

- les organisations criminelles

- des idéologues (politiques ou religieux)

- les services étatiques étrangers

- des employés (ou autres) mécontents

L’ETAT DE LA MENACE

II. risques et actualités

Profils des attaquants

LUCRATIVE
Cyber-mercenaires

IDEOLOGIQUE
Hacktivistes
Cyber-terroristes
Cyber-patriotes

ÉTATIQUE
Unités spécialisées

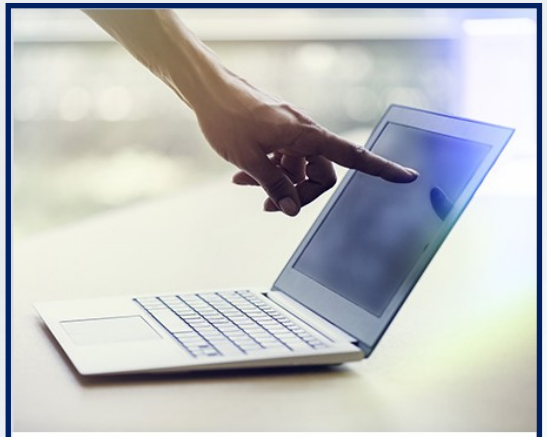
LUDIQUE
Attaquants sans connaissances techniques (script-kiddies)

TECHNIQUE
Hackers chevronnés
Développeurs

PATHOLOGIQUE
Vengeurs
Employés mécontents

Les Menaces

Attaque crapuleuse



Atteinte à l'image

Espionnage

Sabotage

Phishing **Rançongiciel** **escroqueries**	**Dénis de service** **Défacement** **Désinformation**	**Piratage** **Social Engineering** **Spear phishing..**	**Panne organisée**

Attaques les plus populaires

<u>Que recherchent principalement les pirates</u> ?

1 – Informations

2 - Données personnelles (empreinte numérique)

3 - Argent

4 - Réseau de bots (attaques/crypto-mining)

5 - Troubler l'ordre public (*sabotage, désinformation etc.*)

Attaques les plus populaires

Types d’attaques les plus courantes

1 – Phishing / pièce jointe piégée (ou lien web)

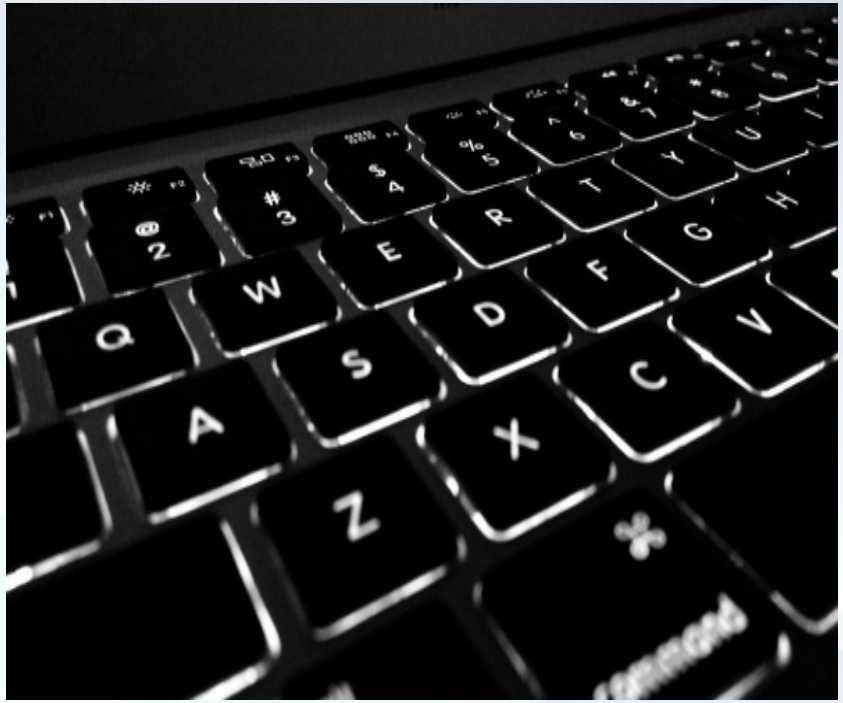
2 – Rançongiciels

3 – usurpations d’ID (président…)

4 – escroquerie aux sentiments, à l’héritage, etc.

5 – Wifi Public / Vulnérabilités / accès non-sécurisés

6 – Clé USB (intrusion consentie ou non)



Ampleur du phénomène : France 2020

CHIFFRES CLÉS 2020 TPE/PME

EN 2020

Quelle que soit la taille de l'entreprise, la menace qui provoque le plus de dégâts est l'attaque informatique par rançongiciel suivi du vol d'identifiants.[3]

43%

des victimes de violations de données étaient des PME.[2]

84%

des PME ont mis en place une formation de sensibilisation à la cybersécurité obligatoire.

1 SUR 5 entreprise Française

ayant subi une attaque a versé une rançon. Les petites entreprises, plus vulnérables, sont les moins bien préparées.[4]

Coût de la cybercriminalité dans le monde en 2020

8,2[1] milliards d'euros

L'Ampleur du phénomène : France 2020

Quelles sont les motivations des cybercriminels ?[5]

- Gains financiers dans 45% des cas d'attaques informatiques.
- Vol de données dans 30% des cas d'attaques informatiques.

Quelles sont les techniques préférées des cybercriminels ?[6]

- La fraude au faux fournisseur.
- La fraude au faux président .
- Les usurpations d'identité (banques, avocats, commissaires aux comptes).
- La fraude au faux client.

2020 : L'ANNÉE DE LA COVID-19

- Aucune explosion majeure des cyberattaques constatée à l'exception des attaques informatiques par ransomware qui touchent surtout les grandes entreprises.
- Les attaques utilisant la COVID-19 comme objet restent marginales puisqu'elles représentent moins de 2% des attaques relevées au mois d'avril.
- La crise sanitaire a mis les technologies d'accès à distance à l'honneur : + 41% pour les solutions VPN, recours massif au Cloud, etc.
- 57% des RSSI français reconnaissent que l'adoption du télétravail a rendu les systèmes d'information plus vulnérables aux cyberattaques.

L'Ampleur du phénomène : France 2021

LES CHIFFRES CLÉS DE LA CYBERSÉCURITÉ

Boutique box internet

54 % des entreprises françaises attaquées en 2021 (1)

+255% d'attaques par ransomware en 2020 par rapport à 2019 (2)

+400% de tentatives de phishing durant le début du confinement (3)

20% des entreprises ont été touchées par un ransomware (1)

50 000€ c'est le coût médian d'une cyberattaque (4)

27% de perte moyenne sur le chiffre d'affaires pour les PME en France (4)

47% des télétravailleurs se font fait piéger par un phishing (1)

73% des entreprises déclarent le phishing comme vecteur d'entrée principal pour les attaques subies (1)

40% des entreprises ont investi dans leur cybersécurité en 2021 (4)

55% des entreprises considèrent que le niveau de menaces en matière de cyberespionnage est élevé (1)

SOURCES : (1) BAROMÈTRE DE LA CYBERSÉCURITÉ EN ENTREPRISE CESIN 2022 - (2) ANSSI - (3) CYBERMALVEILLANCE.GOUV.FR. - (4) STOÏK

PME et cyberattaques

60 % des victimes sont des PME

2/3 des TPE fermeront leurs portes dans les 6 mois après une cyber attaque

+58% d'attaques de mobiles en 2021 par des malwares

source : ANSSI

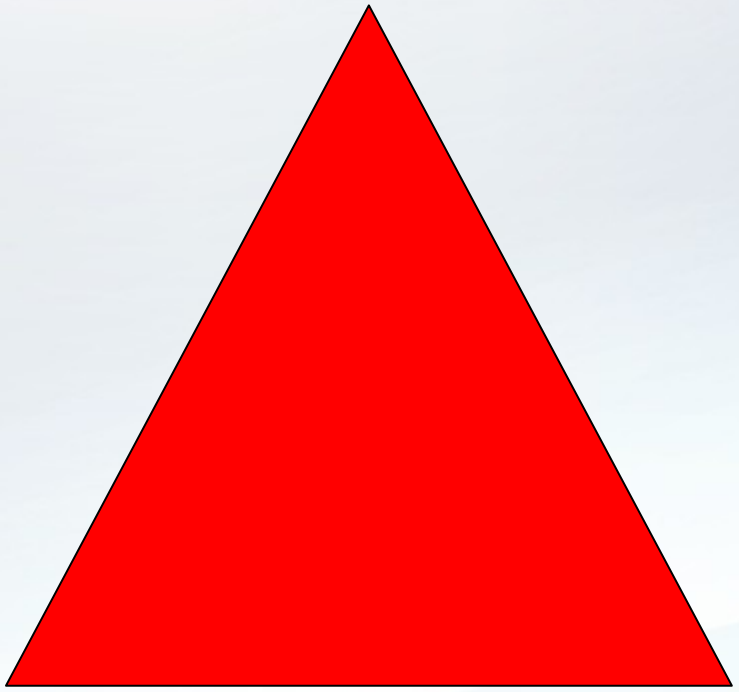
Les mesures de sécurité

VULNÉRABILITÉS

- technique : 10 %

- organisationnelle : 30 %

- humaine : 60 %



ACTIONS CORRECTIVES

- audit sécurité des systèmes d'information

- renforcement des procédures de contrôle interne

- sensibilisation des équipes, formation interne

L’ETAT DE LA MENACE

III. les acteurs de la lutte

Structure judiciaire en place

- TJ PARIS – JIRS - Parquet Cybercriminalité centralisé et spécialisé

– Sous Direction de Lutte contre la Cybercriminalité (**SDLC** - Police Judiciaire) 2015

- Préfecture de Police de Paris (**BEFTI** – Police Judiciaire)

- Directions Zonales de Police Judiciaire (579 ICC – 15 LIONs)

- Signalements internet (PHAROS) = 289 590 signalements en 2020 (tout cas confondus)

- **EUROPOL** (EC3 – European Cybercrime Center) / **EUROJUST** (et Interpol)

- Gendarmerie : Centre de lutte contre les criminalités numériques (**C3N**)
  Section opérationnelle de lutte contre les cybermenaces (**SOLC**)

- DGSI

structures impliquées dans la lutte

- **ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information), CNIL

- www.cybermalveillance.gouv.fr

- Préfet / antenne locale de Sécurité Civile et référents locaux

- DGSE / DRM

- Gendarmerie : Les référents Sécurité Économique et Protection des Entreprises (**SEcoPE**)

- Acteurs privés et civils, associations...

- le **RESEAU DES REFERENTS CYBERMENACE**

structures impliquées dans la cyber

LE RÉSEAU DES RÉFÉRENTS CYBERMENACES

Un réseau de professionnels partenaires, publics et privés, au service du tissu économique local.

3 AXES OPÉRATIONNELS STRATÉGIQUES

AXE 1

Une équipe déployée sur tout le territoire national, associant des commissaires de police des services territoriaux de la police judiciaire, des policiers spécialisés en cybercriminalité, des réservistes opérationnels et citoyens de la Police nationale sur des missions d'experts en prévention ainsi que des partenaires privés.

AXE 2

Un dispositif visant à mener des actions de sensibilisation et de prévention auprès des entreprises sur les risques liés à la cybercriminalité.

AXE 3

Un accompagnement des victimes de cyberattaques en leur prodiguant les premiers gestes de sauvegarde des intérêts de l'entreprise et une orientation vers les services de police pour faciliter le dépôt de plainte et le recueil des preuves numériques.

LA MISE EN ŒUVRE DU RÉSEAU

Par qui ?

Le réseau est constitué :

- Du référent cybermenaces, commissaire de police de la DZPJ/DTPJ.
- De réservistes de la Police nationale issus du monde de l'entreprise: chef d'entreprise, cadre salarié, responsable de la sécurité des systèmes d'information.
- De partenaires privés (notamment commissaires aux comptes).

Avec l'appui de nombreux acteurs et de leurs réseaux : préfet de la zone de défense et de sécurité, CNCC, ANSSI, CNIL, FBF, etc.

Pour qui ?

Le réseau s'adresse principalement :

- à l'ensemble des directions de la Police nationale présentes sur le territoire national;
- aux TPE/PME.

EUROPOL

EUROPEAN MONEY MULE ACTION LEADS TO 1 803 ARRESTS

01 Dec 2021

Press Release

Investigation reveals money mules were laundering profits from online fraud schemes such as business email compromis
Forex scams.

I oday saw the conclusion of the anti-money mule operation EMMA 7, an international action coordinated by Europol in cooperation with 26 countries, I
INTERPOL, the European Banking Federation (EBF) and the FinTech FinCrime Exchange. The operation resulted in 1 803 arrests and the identificatior
18 000 money mules. It also revealed that money mules were being used to launder money for a wide array of online scams such as sim-swapping, ma
middle attacks, e-commerce fraud and phishing.

Over roughly two and a half months of operations, EMMA 7 saw law enforcement, financial institutions and the private sector, including Western Union,
Microsoft and Fourthline, cooperate in a concerted effort against money laundering in Europe, Asia, North America, Colombia and Australia. As well as t
the laundering of profits through money muling networks, investigators also sought intelligence on the sources of these illicit profits, shedding more ligh
size and nature of the criminal economies that money mules serve.

Results from 15 September – 30 November

- 18 351 money mules identified;
- 324 recruiters/herders identified;
- 1 803 arrested individuals;
- 2 503 investigations initiated;
- 7 000 fraudulent transactions reported;
- €67.5 million prevented losses.

ACTIVITÉ JUDICIAIRE

POLICE NATIONALE · DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

INFRACTIONS ÉCONOMIQUES ET FINANCIÈRES – Démantèlement d'un réseau d'escrocs usurpant les qualités de sociétés existantes pour commander des marchandises de toutes sortes (préjudice de plusieurs millions d'euros) –15 interpellations - 60 000 euros saisis

30 novembre 2021

DIFFUSION RESTREINTE

Par SudOuest.fr avec AFP
Publié le 01/12/2021 à 22h19

S'ABONNER

Le système, aux multiples ramifications, visait à blanchir de l'argent obtenu notamment grâce à des arnaques aux faux virements

Un réseau criminel sophistiqué, dont la tête pensante a été interpellée la semaine dernière en Israël, a blanchi en deux ans au moins 16,5 millions d'euros obtenus grâce à des escroqueries aux faux virements, a-t-on appris mercredi de source policière.

L'enquête, menée par l'Office central pour la répression de la grande délinquance financière (OCRGDF), démarre en avril 2019 par l'interpellation à Paris d'un homme de 32 ans, en possession de 900 000 euros en espèces.

« On s'est très rapidement rendu compte que l'on avait affaire à un système de blanchiment et d'escroqueries commises en bande organisée », explique la commissaire divisionnaire Anne-Sophie Coulbois, patronne de l'OCRGDF. Une information judiciaire est alors ouverte par la juridiction interrégionale spécialisée (Jirs) de Paris, chargée des dossiers les plus complexes.

coordonnées

- DTPJ de LIMOGES
  dtpj-limoges@interieur.gouv.fr
  05 55 14 32 00

- Capitaine Gilles ETIENNE
  Division Economique et Financière - investigateur en cybercriminalité
  gilles.etienne@interieur.gouv.fr
  05 55 14 32 79 et 06 79 30 72 77 (pro)

SecNumeco
ANSSI

Témoignage et retours d'expériences

Henri Bois, DISSE Limousin, DREETS Nouvelle-Aquitaine
Gilles Etienne, Spécialiste Cyber Police Nationale
avec le témoignage de **Elysabeth Benali-Léonard**, Chef d'entreprise

Organisé par :

ALIPTIC

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Liberté Égalité Fraternité
Direction générale des Entreprises

Avec le soutien de :

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE
Liberté Égalité Fraternité

RÉGION Nouvelle-Aquitaine

Limoges Métropole
Communauté urbaine

En collaboration avec :

MINISTÈRE DE L'INTÉRIEUR
Liberté Égalité Fraternité

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE Nouvelle-Aquitaine

CLUSIR #Aquitaine

Université de Limoges

ADI Nouvelle-Aquitaine
Agence de Développement et d'Innovation

CCI LIMOGES HAUTE-VIENNE

E.S.T.E.R Limoges Technopole

DIGITAL AQUITAINE

En partenariat avec :

les acteurs de la compétence Nouvelle-Aquitaine

ALLISNA

ALPHA RLH

avrul

cpme 87 HAUTE-VIENNE

CRYPTIS

FIBOIS NOUVELLE AQUITAINE

Gendarmerie nationale

LIMOGES BUSINESS +++CLUB

Mouvement des Entreprises de France Limousin

PÔLE EUROPÉEN DE LA CÉRAMIQUE

POLICE NATIONALE

UIMM LA FABRIQUE DE L'AVENIR

xlim

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

PHISHING

- Comprendre
- Reconnaitre
- Eviter
- Réagir

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Comprendre

L'hameçonnage (phishing en anglais)est une technique frauduleuse destinée à leurrer un utilisateur pour l'inciter à communiquer des données personnelles ou à verser de l'argent en se faisant passer pour un tiers de confiance.

Il peut prendre la forme d'un courriel, d'un SMS, d'un lien web invitant un utilisateur à renseigner son mot de passe ou l'identifiant de son compte d'accès à une application, en usurpant l'identité d'un service existant

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Reconnaitre

Plusieurs critères permettent de reconnaitre un message d'hameçonnage:

Le message revêt un caractère impérieux , intime ou inhabituel.

Le message comporte des erreurs d'orthographe , de style, ou appartient à une autres sphère sociale (ex: message privé sur votre boite professionnelle)

Le message est envoyé par un expéditeur inhabituel, il contient un lien inconnu, une pièce-jointe inattendue ou vous demande votre mot de passe

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Eviter

Afin d'éviter une attaque par hameçonnage, il convient d'adopter les mesures de prévention suivantes:

Adoptez une posture critique.

N'hésitez pas à faire part de vos doutes en contactant votre RSSI

Ne fournissez jamais, sous aucun prétexte, votre mot de passe à un tiers

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Réagir

- Si vous êtes victime d'une attaque par hameçonnage ou en cas de doute:
- **1.Contacter** le responsable de la sécurité des systèmes d'information et **transmettez lui le message**
- **2.Modifier le mot de passe** dés que possible. Veillez également à modifier ce mot de passe s'il est utilisé sur d'autres comptes.
- **3.Conserver le message frauduleux**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Témoignage PHISHING

Une entreprise de Nouvelle-Aquitaine spécialisé dans l'impression a découvert que certain de ses fichiers graphiques avaient été cryptés.

La personne qui a découvert ce cryptage était en télétravail à l'extérieur.

Il a essayé d'ouvrir un fichier word qui avait été renommé et n'y ai pas parvenu.

Ce salarié a alerté immédiatement le responsable informatique de l'entreprise permettant de détecter assez tôt la rentrée sur le réseau du logiciel de cryptage et d'interrompre ainsi sa diffusion en déconnectant les ordinateurs du réseau et de l'internet.

Le responsable informatique a immédiatement fait une alerte à la CNIL (commission nationale de l'informatique et des libertés) et a porté plainte auprès des services du ministère de l'intérieur.

Il a fait intervenir son opérateur internet (orange cyber défense) et a constaté que seul les fichiers word, graphiques et bureautiques ainsi que les procédures qualité et fiches techniques de produits avaient été cryptés)

Les fichiers de productions n'ayant pas été touchés celle-ci a pu continuer dans des conditions normales.

Suite à cette attaque l'entreprise a du recréer ses fichiers manquants et investir dans des matériels tel le boitier spécialisé qui récence les flux de données et analyse les adresses IP de connexion pour déterminer celles qui sont nuisibles ou pas.

Le cloud de l'entreprise n'a lui pas été attaqué.

Mais les sauvegardes internes et externes dans l'entreprise et chez le prestataire de service de l'entreprise ont été cryptées

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Témoignage PHISHING

L'entreprise a aussi mis en place un logiciel qui limite à trois tentatives les essais de casse des mots de passe. Ceci comme pour les cartes bancaire empêche les attaques en force brute.

Pour éviter les attaques par mail elle s'est équipé d'un logiciel (mail in black), qui filtre les bons et mauvais mails et les attaques de bots en analysant la provenance du serveur et l'adresse IP d'envoi

Toutes ces mesures ont considérablement limités les intrusions et renforcer la sécurité du réseau de l'entreprise

Ces mesures s'accompagnent de la formation des agents.

Deuxième témoignage d'une attaque par Phishing

Une entreprise de production de nouvelle aquitaine qui travaille beaucoup avec des clients étrangers utilise les réseaux sociaux pour commercialiser ses produits.

Il y a quelques mois, comme chaque jour quand le chef d'entreprise a voulu ouvrir son compte pour voir quels clients l'avait contacté et s'est vu refuser son accès au réseau social.

Dans la foulée il a reçu une demande de rançon qu'il a refusé de payer.

Renseignement pris auprès de sa secrétaire il a compris que celle-ci avait reçu d'un faux client une réclamation

Avec un lien pour répondre qui l'a amené vers un site miroir frauduleux du réseau social.

Celle-ci a tapé alors les codes d'accès qui ont permis aux hackers de les changer et de prendre le contrôle du site.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Témoignage PHISHING

Le chef d'entreprise a essayé par la suite de contacter le siège social de son hébergeur qui ne l'a pas reconnu comme le propriétaire du site mais comme un usurpateur.

De guerre lasse il a créé un nouveau site d'hébergement avec un mot de passe et des conditions d'accès propriétaire beaucoup plus solides et plus complexes afin de recréer tout son fichier client.

Les hackers propriétaires de l'ancien site ont essayé sans succès de l'utiliser pour vendre de la drogue puis pour se faire passer pour l'entreprise et prendre des commandes avec acomptes payés en bitcoins.

Le ministère de l'intérieur saisi de l'affaire a lancé une réquisition auprès de l'opérateur étranger et a fait fermé l'ancien site.

L'image de l'entreprise a été impactée notamment en matière de communication et mettra du temps à récupérer son rayonnement.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Témoignage PHISHING

Phishing de l'entreprise la saveur des cépages

1er étape il reçoit un mail de sa banque avec une charte graphique conforme en tout point à celle de sa banque. Il ne fait pas attention et confirme ses codes personnel sur le faux de sa banque.

2ème étape Très rapidement il constate sur son compte 4 virements d'un peu plus de 4000 € pour un total d'environ 18 000€

3ème étape il dépose plainte au commissariat de Cognac après avoir demandé le « recall » à sa banque. La police judiciaire de Limoges est saisie sans délais. Immédiatement l'enquêteur en charge du dossier demande les documents d'ouverture des comptes crédités et les solde.

Conclusion

La rapidité d'exécution est fondamentale surtout dans le cas de virement

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Arnaque au président comprendre

*La "Fraude au **président**" consiste pour des escrocs à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision de contrat ou autre*

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Reconnaitre

- Les escroqueries au président sont organisés par des personnes qui ont étudiés durant de longues périodes l'entreprises qu'ils vont attaquer.
- Qui dans l'entreprises possède la capacité de faire des transferts d'argent ?
- Parmi ces personnes qui sont les plus naïves fragiles ou influençables; qui sont les maillons faibles ?
- Les demandes de transferts d'argent se font généralement la veille d'une long week-end ou d'une période de congés pour éviter les blocages ultérieurs de virement.
- Les demandes viennent du Président (imitation de la voix, connaissance très fine de sa famille, de ses habitudes et des noms et habitudes de ses collaborateurs).
- Ces demandes peuvent se faire avec un mail usurpé du président ou d'un haute responsable hiérarchique.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Eviter

Pour éviter les attaques au président il faut sensibiliser le personnel au demandes de virement ou versements précipités

Il faut mettre en place un protocole d'autorisation double (Président + responsable financier)

Il faut sensibiliser le personnels au versement sur des comptes inhabituels en France ou à l'étranger

Il faut mettre en place avec sa banque un protocole de réponse d'urgence pour un blocage rapide des versements.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Réagir

Si vous êtes victime d'une attaque au président il faut immédiatement bloquer le ou les virements.

Il faut immédiatement porter plainte auprès du ministère de l'intérieur pour escroquerie

Il faut revoir et durcir les protocoles de virement en établissant des seuils de contrôle et en vérifiant auprès de vos clients, fournisseurs et banques les numéros de comptes utilisés par l'entreprise.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Témoignages arnaque au président

Une entreprise de nouvelle aquitaine spécialisé dans le service aux entreprise a été victime d'une attaque en phishing qui a abouti au cryptage de ses fichiers par le groupe russe REVIL.

Cette entreprise a refuser de payer la rançon demandée de plusieurs centaines de milliers d'euros.

Heureusement elle avait fait des sauvegarde journalières qui lui ont permis de récupérer l'intégralité de ses fichiers.

Quelques semaines plus tard la secrétaire du PDG de l'entreprise a reçu le mail suivant destiné au responsable de région ,après un appel téléphonique par une personne se faisant passer pour le président.

adresse correct

Vrai adresse entre parenthèse fausse

De : Le PRESIDENT le.president@i .fr <le.president@e.mail.fr>
Envoyé : mardi 11 octobre 2022 09:44
À : XXXXXX XXXXXX (FR - IE Bordeaux) <xxxxxxxx.xxxxxxxxx@ r>
Objet : Dossier en cours

Bonjour,

Je viens de raccrocher avec Me du cabinet KPMG qui me confirme avoir pris contact par téléphone, je pensais avoir envoyé les éléments ce matin pour ce dossier.

Voici l'OPA en cours, nous effectuons en ce moment une opération financière concernant une fusion/acquisition de société basée en Europe.
Ce dossier doit rester strictement confidentiel, personne d'autre ne doit être au courant pour le moment.

L'annonce publique de cette OPA aura lieu le jeudi 20 octobre 2022 dans nos locaux avec la présence de toute l'administration.

Merci de reprendre contact avec KPMG à l'attention de Me pour la remise des coordonnées bancaires afin d'effectuer le virement ce matin.

Contact: .kpmg@consultant.com

Ps: par mesure de sécurité, merci de me contacter uniquement sur mon mail sécurisé (le.president@e.mail.fr) pour cette opération confidentielle où nous pourrons discuter sans risque de divulgation afin de respecter la norme de cette OPA.

Merci de ne me faire aucune allusion sur ce dossier de vive voix, ni même par téléphone uniquement sur mon mail personnel selon la procédure imposée par l'AMF (Autorité des Marchés Financiers).

Cordialement,

Le PRESIDENT

Témoignages arnaque au président

L'en tête était bonne mais la véritable adresse mail écrite entre parenthèse était fausse ainsi que les coordonnée de KPMG , et le soit disant mail sécurisé du président.

A la fin du mail suivant une demande de virement était faite.

La secrétaire a immédiatement alerté le RSSI qui alerté sa hiérarchie.

Depuis de nombreuses attaques simulés ont été organisé par le RSSI pour former le personnel et aboutir à un taux de réponse positive aux attaques, proche du zéro.

L'entreprise suite à ces différentes attaques en a subit plus de 20 par semaine pendant quelques semaines.

Depuis le niveau de sécurité a été fortement relevé.

AUTRE TYPES D'ATTAQUES


Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

CONCLUSION

SecNumeco
ANSSI

Pause déjeuner - Reprise des conférences à 14h

Organisé par :

ALIPTIC

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Liberté Égalité Fraternité
Direction générale des Entreprises

Avec le soutien de :

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE
Liberté Égalité Fraternité

RÉGION Nouvelle-Aquitaine

Limoges Métropole
Communauté urbaine

En collaboration avec :

MINISTÈRE DE L'INTÉRIEUR
Liberté Égalité Fraternité

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE Nouvelle-Aquitaine

CLUSIR #Aquitaine

Université de Limoges

ADI Nouvelle-Aquitaine
Agence de Développement et d'Innovation

CCI LIMOGES HAUTE-VIENNE

E.S.T.E.R
LIMOGES TECHNOPOLE

DIGITAL AQUITAINE

En partenariat avec :

les acteurs de la compétence Nouvelle-Aquitaine

ALLISNA

ALPHA RLH

avrul

cpme 87 HAUTE-VIENNE

CRYPTIS

FIBOIS NOUVELLE AQUITAINE

Gendarmerie nationale

LIMOGES BUSINESS +++CLUB

Mouvement des Entreprises de France Limousin

PÔLE EUROPÉEN DE LA CÉRAMIQUE

POLICE NATIONALE

UIMM LA FABRIQUE DE L'AVENIR

xlim

SecNumeco
ANSSI

Conférence

SÛRETÉ & SÉCURITÉ ÉCONOMIQUE GLOBALE DES ENTREPRISES ET CONFORMITÉ RGPD

Jean-Michel Lathière, Auditeur Cyber IntelliE

Organisé par :

ALIPTIC

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Liberté Égalité Fraternité
Direction générale des Entreprises

Avec le soutien de :

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE
Liberté Égalité Fraternité

Région Nouvelle-Aquitaine

Limoges Métropole
Communauté urbaine

En collaboration avec :

MINISTÈRE DE L'INTÉRIEUR
Liberté Égalité Fraternité

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE
Nouvelle-Aquitaine

CLUSIR #Aquitaine

Université de Limoges

ADI Nouvelle-Aquitaine
Agence de Développement et d'Innovation

CCI LIMOGES HAUTE-VIENNE

E.S.T.E.R
LIMOGES TECHNOPOLE

DIGITAL AQUITAINE

En partenariat avec :

les acteurs de la compétence Nouvelle-Aquitaine

ALLISNA

ALPHA RLH

avrul

cpme 87 HAUTE-VIENNE

CRYPTIS

FIBOIS NOUVELLE AQUITAINE

Gendarmerie nationale

LIMOGES BUSINESS +++CLUB
LA FORCE D'UN RÉSEAU

Mouvement des Entreprises de France Limousin

PÔLE EUROPÉEN DE LA CÉRAMIQUE

POLICE NATIONALE

UIMM LA FABRIQUE DE L'AVENIR

xlim

Une meilleure sécurité pour une plus grande compétitivité

Sûreté & Sécurité Économique globale des Entreprises et Conformité RGPD

Jean-Michel LATHIERE

INTELLIE

Gendarmerie

Entreprise INTELLIE

DPO certifié APAVE et AFNOR

référencé plateforme cybermalveillance

Des attaques de plus en plus nombreuses

En France

1 entreprise française sur 2 est victime d'une attaque informatique

En Europe

1 entreprise allemande sur 2 est victime d'attaques, représentant un préjudice de 15 à 20 milliard d'€ (source service de renseignements allemands)

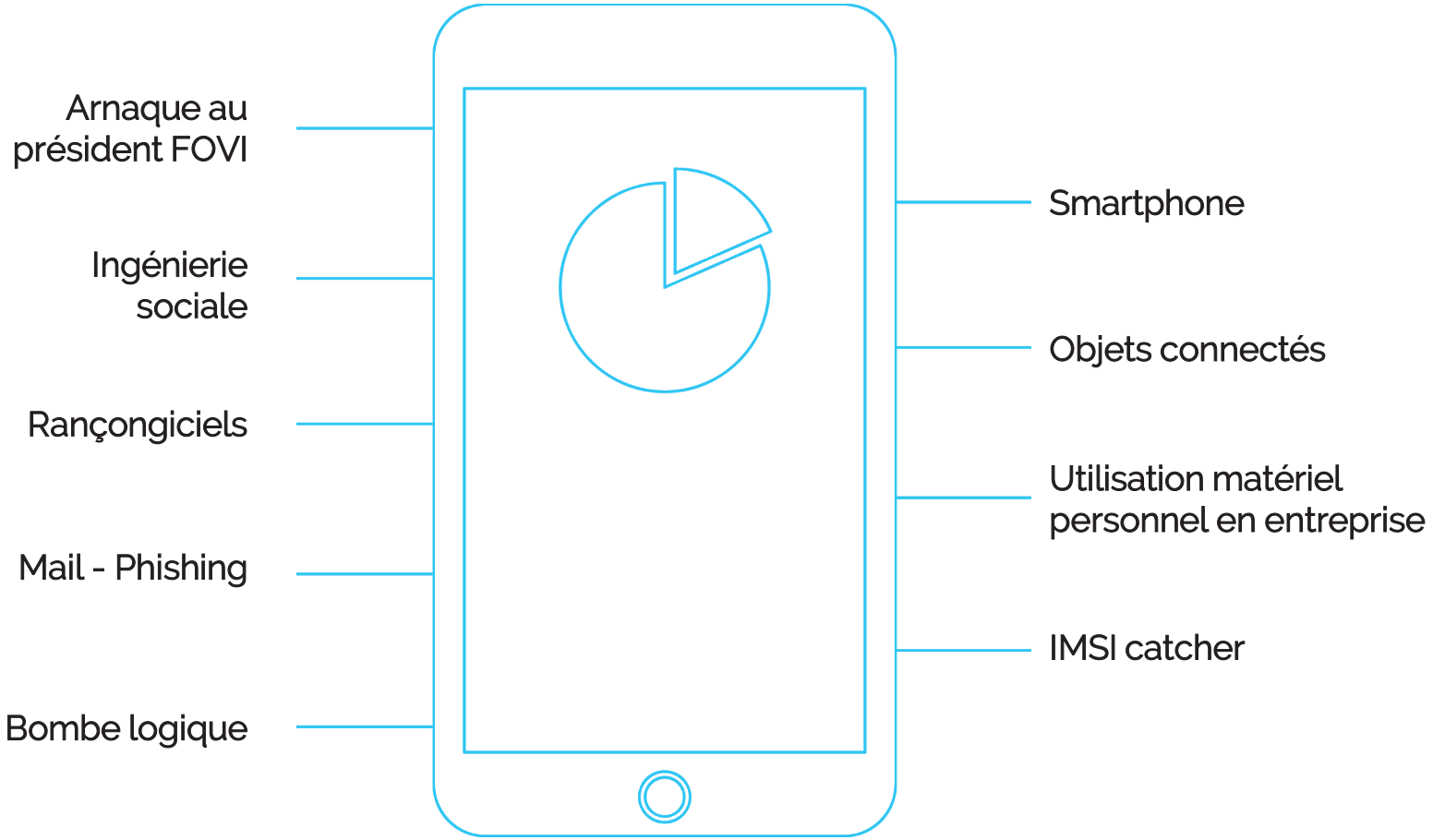
Dans le monde

Le cabinet d'étude PWC estime à 177.300 le nombre de cyberattaques quotidiennes à travers le monde

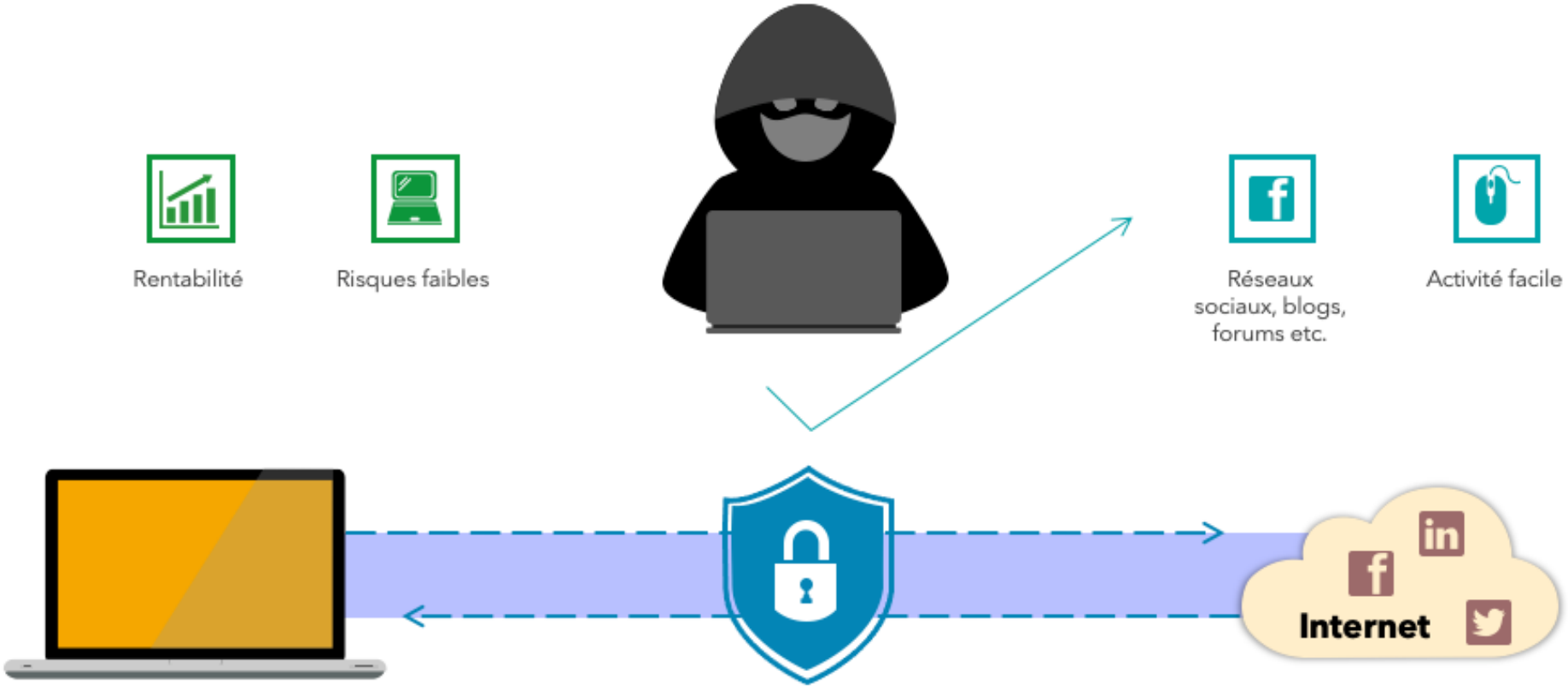
PME

Les PME sont les plus touchées !

Types d'atteintes informatiques des entreprises



Cybercriminalité : encore en forte progression



Bonnes pratiques RGPD

Le RGPD vous aide à savoir où sont les données de votre structure (principalement celles à caractère personnel) et vous aide à les protéger

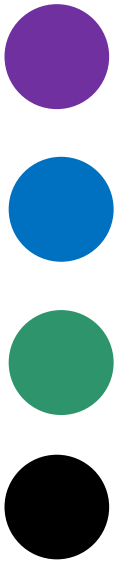
Ordre du jour RGPD

QUESTIONNAIRE

OBJECTIF DE L'ATELIER – LES BASES

COMMENT FAIRE

LES 6 ETAPES CLES ET
LES 8 RÈGLES D'OR



QUESTIONNAIRE

QUESTIONS RGPD

LIEN TEST :https://qruiz.net/Q/?LwGP1A

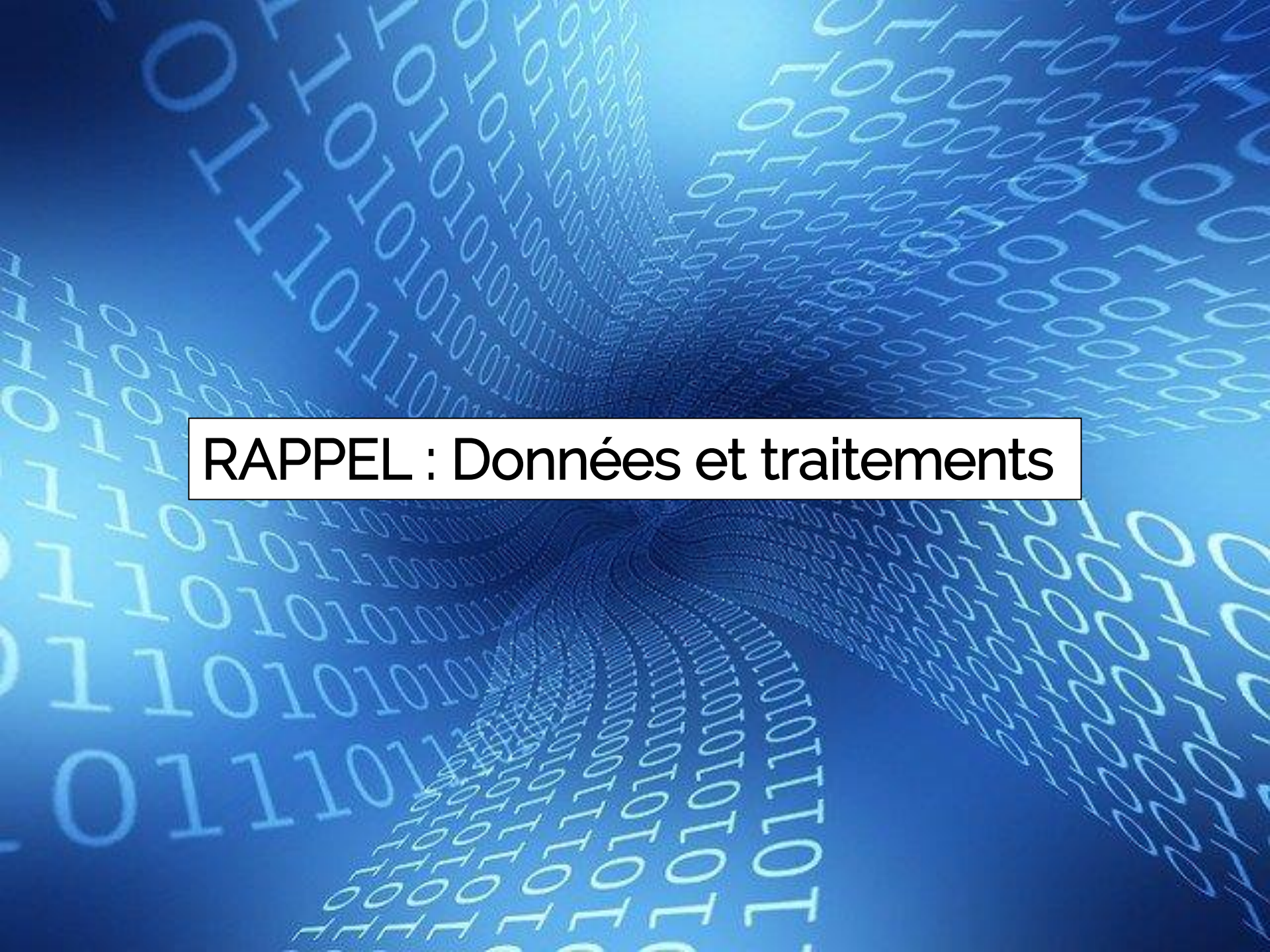
QUESTIONS RGPD

Questions	Réponses			
1/ Quels sont les principes relatifs au traitement des données à caractère personnel ? (Plusieurs bonnes réponses possibles)	Les données collectées doivent être adéquates, pertinentes et limitées à ce qui nécessaire au regard des finalités	Exactes et si nécessaire, tenues à jour	Collectées pour des finalités non déterminées, non explicites et non légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités	Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités
2/ Combien existe-t-il de bases juridiques pour qu'un traitement soit licite ?	2	4	6	8
3/ En France, à quel âge est fixé la collecte des données sur les mineurs sans l'accord parental ?	11	12	13	15
4/ Dans le strict sens du RGPD, quel traitement de données à caractère personnel ne fait pas partie de données dites sensibles ?	Les opinions religieuses	Les données génétiques	Les données liées à la santé	Les données bancaires
5/ indiquez quelles sont les conditions pour qu'un traitement de données sensibles ne soit pas interdit ? (Plusieurs bonnes réponses possibles) ?	La personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques	Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique	Le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée	Le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi

REPONSES RGPD

Questions	Réponses			
1/ Quels sont les principes relatifs au traitement des données à caractère personnel ? (Plusieurs bonnes réponses possibles)	Les données collectées doivent être adéquates, pertinentes et limitées à ce qui nécessaire au regard des finalités	Exactes et si nécessaire, tenues à jour	Collectées pour des finalités non déterminées, non explicites et non légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités	Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités
2/ Combien existe-t-il de bases juridiques pour qu'un traitement soit licite ?	2	4	6	8
3/ En France, à quel âge est fixé la collecte des données sur les mineurs sans l'accord parental ?	11	12	13	15
4/ Dans le strict sens du RGPD, quel traitement de données à caractère personnel ne fait pas partie de données dites sensibles ?	Les opinions religieuses	Les données génétiques	Les données liées à la santé	Les données bancaires
5/ indiquez quelles sont les conditions pour qu'un traitement de données sensibles ne soit pas interdit ? (Plusieurs bonnes réponses possibles) ?	La personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques	Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique	Le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée	Le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi

OBJECTIF DE L'ATELIER – LES BASES



RAPPEL : Données et traitements

Donnée personnelle :

RGPD, ARTICLE 4 : toute information se rapportant à une personne physique identifiée ou identifiable est réputée être une personne physique identifiable ou être indentifiable "DIRECTEMENT ou INDIRECTEMENT" notamment en référence à un identifiant : qui sont ?

le nom,
le prénom,
l'adresse postale,
l'adresse courriel,
les données de localisation etc.

Donnée personnelle sensible (article 9 + ARTICLE 10):
Il s'agit de toutes les informations liées à une personne physique identifiée ou identifiable:

Le traitement des données à caractère personnel qui révèle :
- L'origine raciale ou ethnique
- Les données de santé
- Les opinions politiques
- Les convictions religieuses
- L'appartenance syndicale
- L'orientation sexuelle
- Les données génétiques, biométriques
- *Données particulières sur le NIR*

Les traitements :

Qu'est-ce qu'un traitement de données personnelles ?

Il s'agit de toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données, telles que :
la collecte,
l'enregistrement,
l'organisation,
la structuration,
la conservation,
l'adaptation ou la modification,
l'extraction,
la consultation,
l'utilisation,
la communication par transmission,
la diffusion ou toute autre forme de mise à disposition,
le rapprochement ou l'interconnexion,
la limitation,
l'effacement ou la destruction.

Les traitements :

Qu'est-ce qu'un traitement de données personnelles ?

Exemples :
une base de données ;
un tableau Excel ;
une installation de vidéosurveillance ;
un système de paiement par carte bancaire ou reconnaissance biométrique ;
une application pour smartphone, etc.

Un traitement de données à caractère personnel peut être informatisé ou non.

Qui sont les acteurs des traitements ?

5 acteurs principaux :

- Le Responsable de Traitement (RT) – art 24

- Le Co-Responsable de Traitement (Co-RT) – art 26

- Le Sous-Traitant (ST) – art 28

- Les personnes concernées (PC)

- Le DPO/DPD – art 37, 38, 39

Très important car cela défini le niveau de responsabilité pour ces acteurs

COMMENT FAIRE UNE MISE EN CONFORMITÉ


Les 6 étapes clés

ETAPE 1

DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données.

ETAPE 2

CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

ETAPE 3

PRIORISER LES ACTIONS À MENER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

ETAPE 4

GÉRER LES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD).

ETAPE 5

ORGANISER LES PROCESSUS INTERNES

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

ETAPE 6

DOCUMENTER LA CONFORMITÉ

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

LES 8 RÈGLES D'OR

Les 8 règles d'or du RGPD

1. LICEITE du Traitement :

Un traitement ne peut être mis en œuvre que s'il est fondé sur une des 6 conditions de Licéité :

- - La personne a consenti au traitement pour une ou plusieurs finalités.
- - Le traitement est nécessaire à l'exécution du contrat
- - Le traitement est nécessaire au respect d'une obligation légale à laquelle le RT est soumis
- - Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne
- - Le traitement est nécessaire à l'exécution d'une mission d'intérêt général ou relevant de l'intérêt public.
- - Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le RT.


Les droits des PC


	Droit d'accès Article 15	Droit de rectification Article 16	Droit à l'effacement Article 17	Droit à la limitation du traitement Article 18	Droit à la portabilité Article 20	Droit d'opposition Article 21
Consentement	Oui	Oui	Oui	Oui	Oui	Retrait du consentement
Contrat	Oui	Oui	Oui	Oui	Oui	Non
Obligation légale	Oui	Oui	Non	Oui	Non	Non
Intérêts vitaux	Oui	Oui	Oui	Oui	Non	Non
Intérêt public	Oui	Oui	Non	Oui	Non	Oui
Intérêt légitime	Oui	Oui	Oui	Oui	Non	Oui

Les 8 règles d'or du RGPD

2- FINALITE du traitement :

Traitement pour une finalité définie et légitime.

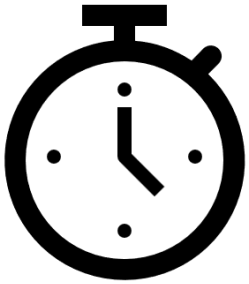
3- MINIMISATION des Données :

Seules les données nécessaires pour atteindre la FINALITE, peuvent être collectées et traitées.

Les 8 règles d'or du RGPD

4- PROTECTION particulière des Données Sensibles :

Les données SENSIBLES peuvent être collectées et traitées uniquement dans certaines conditions.



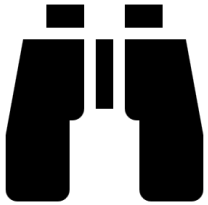
5- CONSERVATION LIMITEE des données :

Doivent être archivées, supprimées ou anonymisées dès que la FINALITE est atteinte.

Les 8 règles d'or du RGPD

6- OBLIGATION DE SECURITE :

Au regard des risques des mesures doivent être mises en œuvre pour s'assurer de la sécurité des données traitées. Mesures techniques et organisationnelles afin de garantir un niveau de sécurité adapté au risque.



7- TRANSPARENCE :

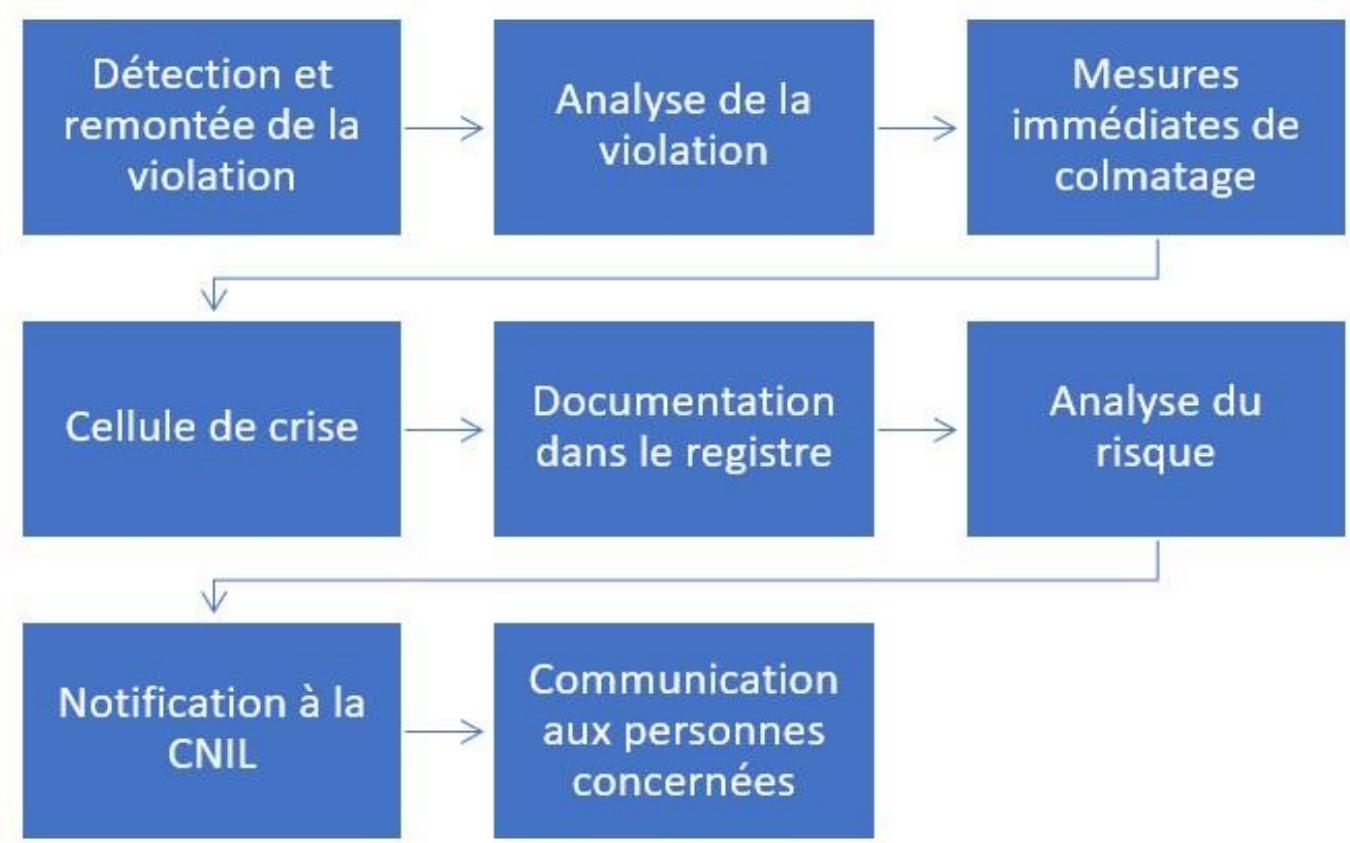
Informer toute personne de l'utilisation des données les concernant et de la manière d'exercer leurs droits

8- DROIT DES PERSONNES :

Elles bénéficient de nombreux droits leur permettant de garder la maîtrise de leurs données.

Exemple schéma demande de droits

Exemple schéma violation de données



Un petit plus : Les 3 questions principales à poser à votre ST

1. Pouvez-vous nous transmettre le contrat article 28 du RGPD ?

2. Combien de personnes ont été formées dans votre entreprise pour gérer les obligations imposées par le RGPD ?

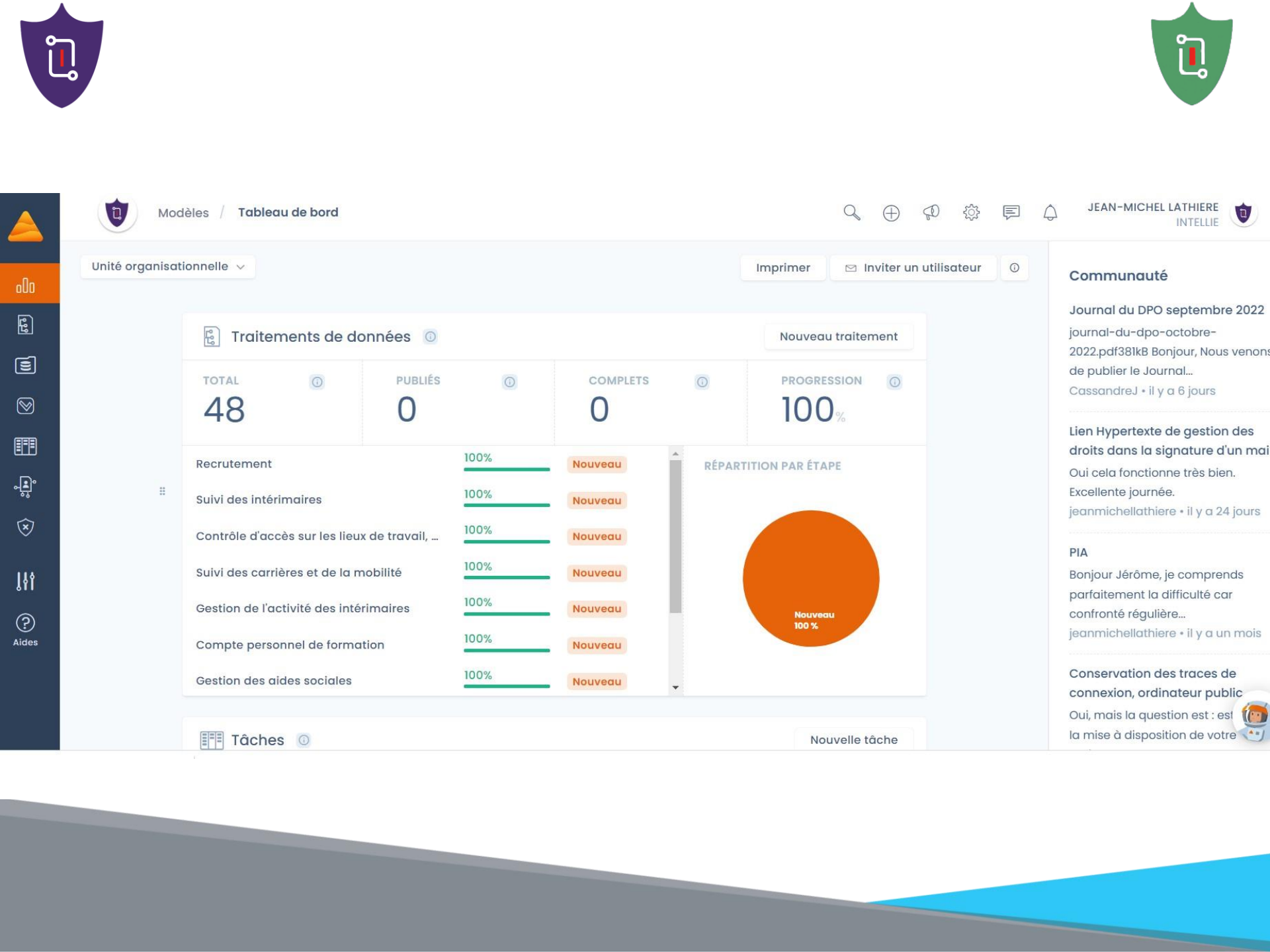
3. Est-ce que vous faites des transferts hors UE ?

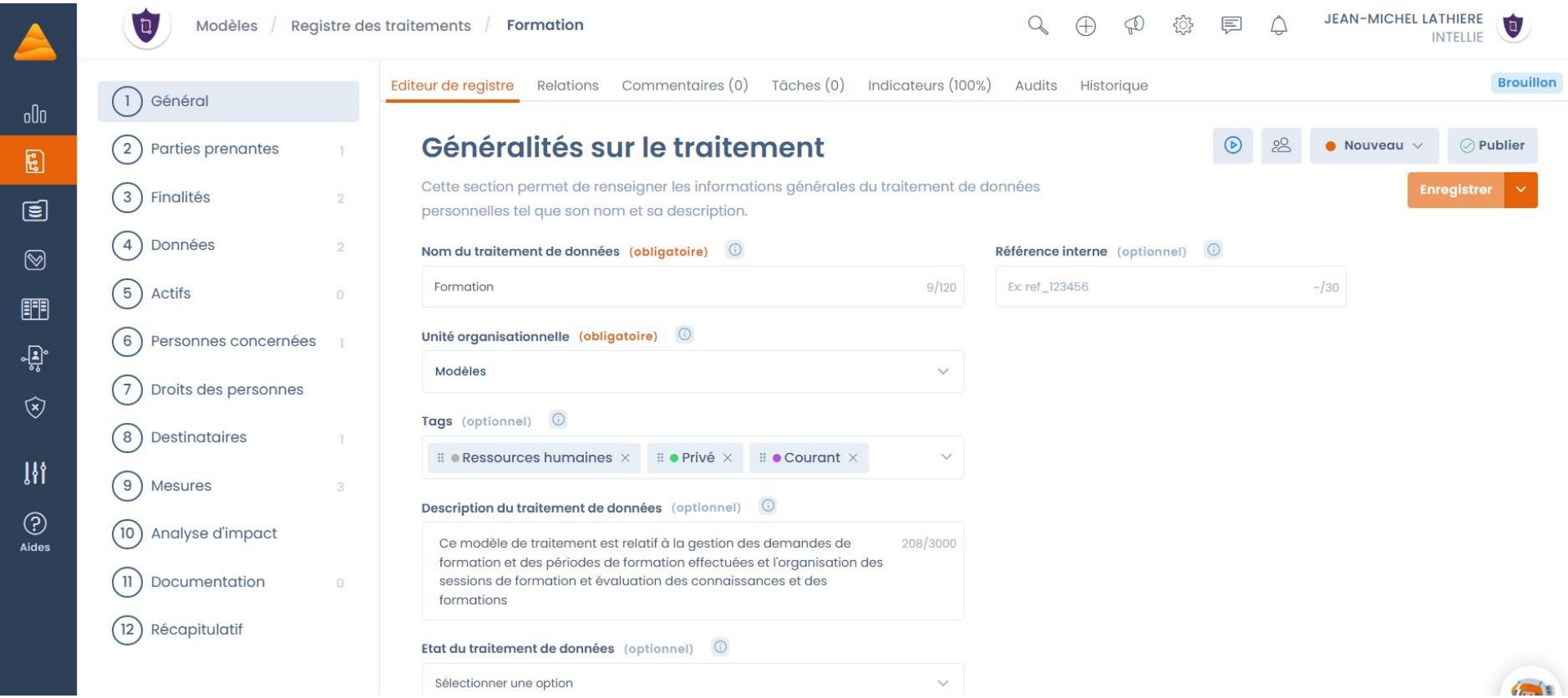
Prospection commerciale

Un deuxième petit plus : la prospection commerciale

TABLEAU RECAPITULATIF
Prospection email : **OPT-*IN***
Prospection SMS : **OPT-*IN***
Transmission, des DCP pour des prospections email : **OPT-*IN***
Prospection postale : **OPT-*OUT***
Prospection par téléphone : **OPT-*OUT***
Transmission des DCP pour des prospections postales et téléphones : **OPT-*OUT***

Exemple : OUTIL CONFORMITE
Registre des traitements


Modèles / Tableau de bord
JEAN-MICHEL LATHIERE
INTELLIE
Aides
Unité organisationnelle
Imprimer
Inviter un utilisateur
Traitements de données
Nouveau traitement
TOTAL
48
PUBLIÉS
0
COMPLETS
0
PROGRESSION
100%
Recrutement 100% Nouveau
Suivi des intérimaires 100% Nouveau
Contrôle d'accès sur les lieux de travail, ... 100% Nouveau
Suivi des carrières et de la mobilité 100% Nouveau
Gestion de l'activité des intérimaires 100% Nouveau
Compte personnel de formation 100% Nouveau
Gestion des aides sociales 100% Nouveau
RÉPARTITION PAR ÉTAPE
Nouveau
100 %
Tâches
Nouvelle tâche
Communauté
Journal du DPO septembre 2022
journal-du-dpo-octobre-2022.pdf381kB Bonjour, Nous venons de publier le Journal...
CassandreJ • il y a 6 jours
Lien Hypertexte de gestion des droits dans la signature d'un mai
Oui cela fonctionne très bien. Excellente journée.
jeanmichellathiere • il y a 24 jours
PIA
Bonjour Jérôme, je comprends parfaitement la difficulté car confronté régulière...
jeanmichellathiere • il y a un mois
Conservation des traces de connexion, ordinateur public
Oui, mais la question est : est la mise à disposition de votre


Modèles / Registre des traitements / Formation
JEAN-MICHEL LATHIERE
INTELLIE
Aides
1 Général
2 Parties prenantes 1
3 Finalités 2
4 Données 2
5 Actifs 0
6 Personnes concernées 1
7 Droits des personnes
8 Destinataires 1
9 Mesures 3
10 Analyse d'impact
11 Documentation 0
12 Récapitulatif
Editeur de registre
Relations
Commentaires (0)
Tâches (0)
Indicateurs (100%)
Audits
Historique
Brouillon
Généralités sur le traitement
Nouveau
Publier
Enregistrer
Cette section permet de renseigner les informations générales du traitement de données personnelles tel que son nom et sa description.
Nom du traitement de données (obligatoire)
Formation
9/120
Référence interne (optionnel)
Ex: ref_123456
-/30
Unité organisationnelle (obligatoire)
Modèles
Tags (optionnel)
Ressources humaines
Privé
Courant
Description du traitement de données (optionnel)
Ce modèle de traitement est relatif à la gestion des demandes de formation et des périodes de formation effectuées et l'organisation des sessions de formation et évaluation des connaissances et des formations
208/3000
Etat du traitement de données (optionnel)
Sélectionner une option

Modèles / Registre des traitements / **Formation**

JEAN-MICHEL LATHIERE
INTELLIE

1. Général
2. Parties prenantes 1
3. Finalités 2
4. Données 2
5. Actifs 0
6. Personnes concernées 1
7. Droits des personnes
8. Destinataires 1
9. Mesures 3
10. Analyse d'impact
11. Documentation 0
12. Récapitulatif

Editeur de registre | Relations | Commentaires (0) | Tâches (0) | Indicateurs (100%) | Audits | Historique

Brouillon

Quelles sont les finalités du traitement ?

Nouveau | Publier

Enregistrer

La finalité d'un traitement est l'objectif principal de l'utilisation des données personnelles. Ces données doivent être collectées pour un but bien déterminé et légitime et ne doivent pas être traitées ultérieurement de façon incompatible avec cet objectif initial.

Ajouter une finalité 2 finalités

1	**Gestion des demandes de formation et des périodes de formation effectuées.**	Contrat ou mesures précontractuelles - art. 6-1 b)
2	**Organisation des sessions de formation et évaluation des connaissances et des formations.**	Intérêts légitimes du responsable du traitement ou d'un tiers - art. 6-1 f) Réponse aux demandes de formation et suivi de la formation par l'employeur.

Retour **Suivant**

Modèles / Registre des traitements / **Formation**

JEAN-MICHEL LATHIERE
INTELLIE

1. Général
2. Parties prenantes 1
3. Finalités 2
4. Données 2
5. Actifs 0
6. Personnes concernées 1
7. Droits des personnes
8. Destinataires 1
9. Mesures 3
10. Analyse d'impact
11. Documentation 0
12. Récapitulatif

Editeur de registre | Relations | Commentaires (0) | Tâches (0) | Indicateurs (100%) | Audits | Historique

Brouillon

Quelles sont les finalités du traitement ?

Nouveau | Publier

Enregistrer

La finalité d'un traitement est l'objectif principal de l'utilisation des données personnelles. Ces données doivent être collectées pour un but bien déterminé et légitime et ne doivent pas être traitées ultérieurement de façon incompatible avec cet objectif initial.

Ajouter une finalité 2 finalités

1	**Gestion des demandes de formation et des périodes de formation effectuées.**	Contrat ou mesures précontractuelles - art. 6-1 b)
2	**Organisation des sessions de formation et évaluation des connaissances et des formations.**	Intérêts légitimes du responsable du traitement ou d'un tiers - art. 6-1 f) Réponse aux demandes de formation et suivi de la formation par l'employeur.

Retour **Suivant**

ALIPTIC

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Direction générale des Entreprises

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE

Région Nouvelle-Aquitaine

Limoges Métropole
Communauté urbaine

En collaboration avec :

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE
Nouvelle-Aquitaine

CLUSIR #Aquitaine

Université de Limoges

ADI Nouvelle-Aquitaine

CCI LIMOGES HAUTE-VIENNE

E.S.T.E.R

DIGITAL AQUITAINE

MERCI POUR VOTRE ECOUTE

jmlathiere@intellie.fr
06.60.24.15.45

INTELLIE

www.intellie.fr

SecNumeco
ANSSI

Conférence

RÉSILIENCE ET CONTINUITÉ D'ACTIVITÉ : PSSI

Pierre Venot, Responsable CLUSIR NA Antenne de Limoges

Organisé par :

ANSSI — ALIPTIC — France IT — Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique — Direction générale des Entreprises

Avec le soutien de :

Préfète de la région Nouvelle-Aquitaine — Région Nouvelle-Aquitaine — Limoges Métropole Communauté urbaine

En collaboration avec :

Ministère de l'Intérieur — Campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine — CLUSIR #Aquitaine — Université de Limoges — ADI Nouvelle-Aquitaine — CCI Limoges Haute-Vienne — E.S.T.E.R — Digital Aquitaine

En partenariat avec :

les acteurs de la compétence Nouvelle-Aquitaine — ALLISNA — Alpha RLH — Avrul — CPME 87 Haute-Vienne — Cryptis — Fibois Nouvelle Aquitaine — Gendarmerie nationale — Limoges Business Club — Mouvement des Entreprises de France Limousin — Pôle européen de la céramique — Police nationale — UIMM La fabrique de l'avenir — Xlim

Présentation SECNUMECO

Résilience et continuité activité

Pierre VENOT

Directeur Sécurité Systèmes d'Information

Groupe PICOTY - AVIA –

Responsable antenne Clusir Limousin

picoty

CLUSIR

Limousin

Comment tendre vers la résilience?

1er SOCLE

INFRA du SI

GOUVERNANCE

La gouvernance pose les bases…

La résilience commence par la gestion de l'humain notamment par des biais réglementaires et documentaires

La PSSI est la politique de Sécurité des Systèmes d'information et permet de donner le cap de la sécurité dans l'entreprise. Elle guide les collaborateurs et fixe les limites (ex mdp, utilisations des supports etc…)

picoty

…L’infrastructure en est la pierre angulaire

Avant de parler de résilience il faut disposer d’éléments composant le SI fiables, sécurisés et cloisonnés.

L’architecture de sauvegarde doit être hermétique et reposer sur différentes technologies (avec différents types de sauvegarde).

Il faut déterminer précisément ce qui doit être sauvegarder. Identifier les éléments les plus importants pour préparer les plans de résilience.

Les analyses de risques sont un prérequis indispensable à la bonne gestion de ces éléments pour **connaitre les activités prioritaires et les fichiers et applications essentiels.**

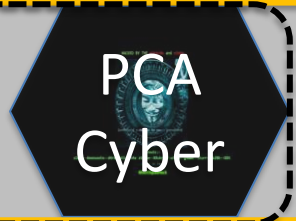
picoty

Comment tendre vers la résilience?

CONTINUITE ACTIVITE

2eme SOCLE

PRA



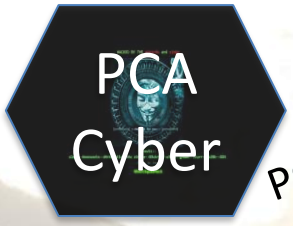
INFRA

GOUVERNANCE

picoty

Comment s'y préparer organisationnellement…

PCA Supports



PCA métiers

- **PCA** = Plan de Continuité d'Activité en cas de défaillance ou panne matériel. Il peut y avoir des Activités prioritaires définies: C'est la haute disponibilité des infrastructures!

- **PCI** = Plan de Continuité informatique; PCA de la DSI ou du service informatique, constitué de l'ensemble des dispositifs/procédures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien des prestations essentielles de la DSI dont la continuité du SI. Et ce le cas échéant, de façon temporaire, en entrainant la reprise planifiée des activités.

  Cela implique de connaitre le(s) système(s) de sauvegarde, les temps de restauration de chacune des phases et les tester!

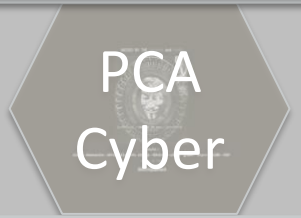
- **PCA Cyber** = PCA Métier en cas d'indisponibilité prolongée du SI à la suite d'une cyberattaque paralysante. Ensemble des procédures et modes **dégradés** qui permettent à l'organisme d'assurer a minima la continuité de ses activités prioritaires sans tout ou partie du SI à travers la planification de solutions métiers dégradées ou alternatives (supports papier, tableaux excel…).

Connaissance des risques!

https://www.economie.gouv.fr/files/hfds-guide-pca-plan-continuite-activite-_sgdsn.pdf

Comment tendre vers la résilience?

OPTIMISATION



INFRA

GOUVERNANCE

picoty

Comment s'y préparer organisationnellement…

↳ Elaborer une procédure de gestion de crise reposant sur les différents plans élaborés.
La procédure doit à minima mentionner la composition de la cellule de crise, les repères spatio-temporels, rôles et missions, communication ou encore annuaires imprimés ou sur supports externes.
Se reposer sur la documentation de l'ANSSI
https://www.ssi.gouv.fr/uploads/2021/12/anssi-guide-gestion_crise_cyber.pdf.

↳ Se documenter et s'informer notamment sur les coûts:
- Coûts de la remédiation
- Coûts de l'arrêt du SI
- Coûts d'une assurance cyber (et difficultés pour y souscrire)
- Couts des évolutions techniques

S'exercer si l'on dispose de la maturité…

picoty

Pour résumer…

Sensibiliser et former

Aux risques cyber sur les différents themes importants:

- Phishing
- Mots de passes
- Réseaux sociaux

Sauvegarder les données

Réaliser différentes sauvegardes en ligne et hors ligne

La resilience et la protection aux menaces

Il s'agit d'un ensemble d'actions permanentes non limitatives.

Se doter d'outils de protection

Antivirus, EDR, Anti Spam, SIEM …

Se preparer à la crise

Connaitre les besoins métiers, se doter de PCA et PRA, procedure de gestion de crise

Respecter les préconisations de l'ANSSI

Le guide d'hygiene informatique et les documentations techniques notamment

Mises à jour régulières

Veille vulnérabilités

Surveillances actives

Des traces internes et externes

picoty

Des questions?

Mes coordonnées:

Pierre VENOT
p.venot@picoty.fr
Antenne-limoges@clusir-aquitaine.fr

CLUSIR
Limousin

picoty

SecNumeco
ANSSI

Table ronde

L'ACTION RÉGIONALE ET TERRITORIALE

Philippe Roches, Chargé de Mission Cybersécurité Région Nouvelle-Aquitaine
Guy Flament, Directeur du Campus Cyber Nouvelle-Aquitaine
Damien Sauveron, Doyen de la FST de l'Université de Limoges
Alexis Mons, Président de l'ALIPTIC

Organisé par :

ALIPTIC

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Liberté Égalité Fraternité
Direction générale des Entreprises

Avec le soutien de :

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE
Liberté Égalité Fraternité

Région Nouvelle-Aquitaine

Limoges Métropole
Communauté urbaine

En collaboration avec :

MINISTÈRE DE L'INTÉRIEUR
Liberté Égalité Fraternité

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE Nouvelle-Aquitaine

CLUSIR #Aquitaine

Université de Limoges

ADI Nouvelle-Aquitaine
Agence de Développement et d'Innovation

CCI LIMOGES HAUTE-VIENNE

E.S.T.E.R
LIMOGES TECHNOPOLE

DIGITAL AQUITAINE

En partenariat avec :

les acteurs de la compétence Nouvelle-Aquitaine

ALLISNA

ALPHA RLH

avrul

cpme 87 HAUTE-VIENNE

CRYPTIS

FIBOIS NOUVELLE AQUITAINE

Gendarmerie nationale

LIMOGES BUSINESS +++CLUB
LA FORCE D'UN RÉSEAU

Mouvement des Entreprises de France Limousin

PÔLE EUROPÉEN DE LA CÉRAMIQUE

POLICE NATIONALE

UIMM LA FABRIQUE DE L'AVENIR

xlim

SecNumeco
ANSSI

Synthèse et Clôture du SecNumEco

Olivier Grall, Délégué à la Sécurité Numérique Nouvelle-Aquitaine ANSSI

Organisé par :

ALIPTIC

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Liberté Égalité Fraternité
Direction générale des Entreprises

Avec le soutien de :

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE
Liberté Égalité Fraternité

RÉGION Nouvelle-Aquitaine

Limoges Métropole
Communauté urbaine

En collaboration avec :

MINISTÈRE DE L'INTÉRIEUR
Liberté Égalité Fraternité

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE Nouvelle-Aquitaine

CLUSIR #Aquitaine

Université de Limoges

ADI Nouvelle-Aquitaine
Agence de Développement et d'Innovation

CCI LIMOGES HAUTE-VIENNE

E.S.T.E.R
LIMOGES TECHNOPOLE

DIGITAL AQUITAINE

En partenariat avec :

les acteurs de la compétence Nouvelle-Aquitaine

ALLISNA

ALPHA RLH

avrul

cpme 87 HAUTE-VIENNE

CRYPTIS

FIBOIS NOUVELLE AQUITAINE

Gendarmerie nationale

LIMOGES BUSINESS CLUB

Mouvement des Entreprises de France Limousin

PÔLE EUROPÉEN DE LA CÉRAMIQUE

POLICE NATIONALE

UIMM LA FABRIQUE DE L'AVENIR

xlim