MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

UNE CYBER ATTAQUE, ÇA N'ARRIVE PAS QU'AUX AUTRES...

Gendarmerie nationale

pôle emploi

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

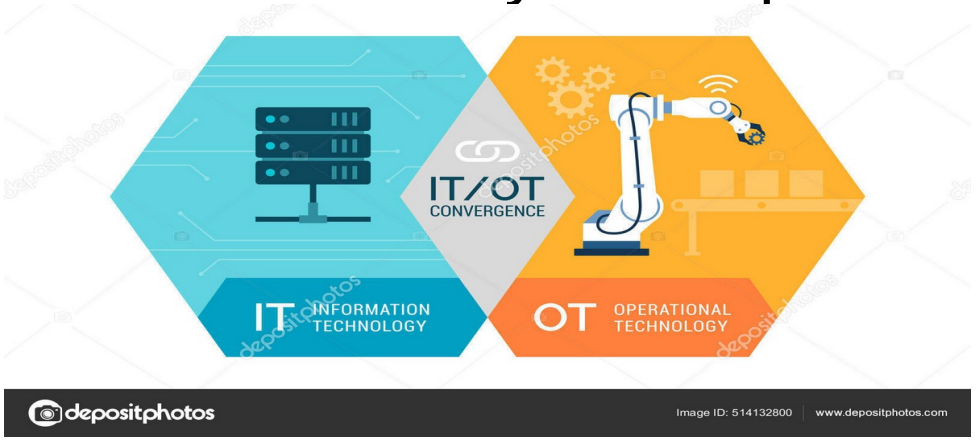
PÔLE MÉTAL 2S
Cluster métallurgique

COMPRENDRE

cybersécurité des systèmes industriels (« Operational Technology ») - OT

La convergence des univers IT (Information Technology) et OT

- levier d'efficacité pour les processus et les métiers.
- mais également un facteur de cyber-risques.



Gendarmerie nationale

pôle emploi

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

FACTEURS DE VULNÉRABILITÉ

- **L'AGE** : parc informatique IT / OT

5 ans / 40 ans

- **Hardware / software** : maintien en condition de sécurité (MCS) / maintien en condition opérationnelle (MCO)

- **L'environnement** : contrôle d'accès moins aisé, conditions (poussière, humidité, températures …)

- **Priorités cyber** : OT → disponibilité, intégrité, confidentialité
  IT → confidentialité, intégrité, disponibilité

Gendarmerie nationale

pôle emploi

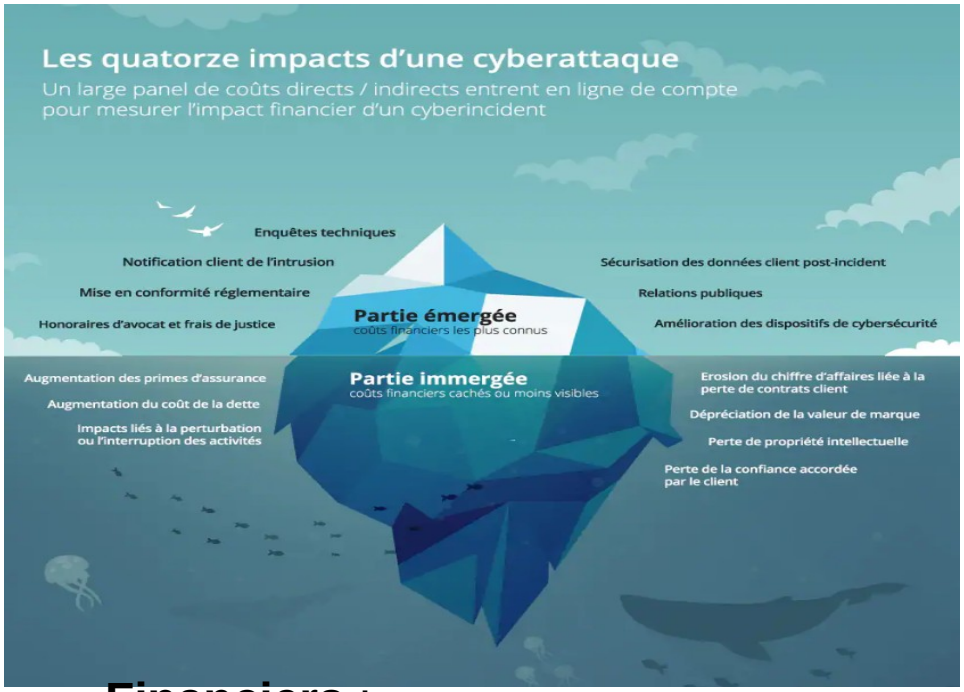
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

COMPRENDRE
LES IMPACTS

Métiers :
- Chaîne de production
- Gestion des stocks
- Qualité et traçabilité
- Économie et emplois

Juridiques :
- Plaintes de clients
- Amendes rgpd / OIV
- Engagement des responsabilités individuelles civile et pénale...



Financiers :
- Rançon si payée
- Remédiation
- Communication
- Perte d'exploitation
- Protection post-crise...

Organisation :
- Perte de données
- Fonctionnement en mode dégradé (plus de messagerie...)

Humains ou matériel :
- Personnels déboussolés, fatigués…
- Retour au fax...

Gouvernance :
- Choix des priorités dans la gestion de la crise sous l'éclairage des techniciens

Gendarmerie nationale

pôle emploi

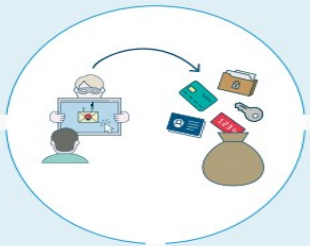
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

HAMEÇONNAGE

On vous incite à communiquer des informations importantes ?
Ne tombez pas dans le piège.

QUE SE PASSE-T-IL ?

1. Vous recevez un courriel piégé
Le courriel suspect vous invite à :
- cliquer sur une pièce-jointe ou un lien piégés
- communiquer des informations personnelles



2. L'attaquant se fait passer pour une personne ou un tiers de confiance
L'attaquant est en mesure de :
- prendre le contrôle de votre système
- faire usage de vos informations

Impact de l'attaque

Intégrité
Disponibilité
Confidentialité
Authenticité

Motivations principales

Atteinte à l'image
Appât du gain
Revendication
Espionnage
Nuisance
Sabotage

COMMENT RÉAGIR ?

Vous êtes victime - Ne perdez pas un instant !

1 - Renouvelez immédiatement les identifiants des comptes compromis

2 - Contactez votre service informatique ou un expert (ou trouvez le vôtre sur www.cybermalveillance.gouv.fr)

3 - Signalez l'incident sur PHAROS (www.internet-signalement.gouv.fr)

4 - Portez plainte auprès des services compétents (www.ssi.gouv.fr/en-cas-dincident)

5 - Plus de conseils avec INFO ESCROQUERIES au 0 805 805 817 (numéro gratuit)

COMMENT SE PROTÉGER ?

Ne tombez pas dans le piège

- Ne cliquez jamais sur un lien ou une pièce-jointe qui vous semblent douteux.
- Ne répondez jamais à un courriel suspect. Au moindre doute, contactez l'expéditeur par un autre canal.
- Évitez l'effet boule de neige ! Disposez d'un mot de passe unique pour chaque application.
- + de conseils avec la CNIL : www.cnil.fr/fr/tag/mots-de-passe
- Vérifiez les paramètres de sécurité de votre compte de messagerie.
- Activez l'authentification à double facteur

En savoir plus sur les attaques par hameçonnage : www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/arnaques-par-message-electronique-comment-identifier-et-dejouer-lhameconnage

Version 2.0 - Janvier 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

PÔLE MÉTAL 2S
Cluster métallurgique

LES INFRACTIONS

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- Escroquerie (article 313-1 du code pénal) : l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.
- Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal) : une telle collecte constitue un délit passible d'une peine d'emprisonnement de cinq ans et de 300 000 euros d'amende.
- Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal) : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.
- Contrefaçon et usage frauduleux de moyen de paiement (articles L163-3 et L163-4 du code monétaire et financier) : délit passible d'une peine d'emprisonnement de sept ans et de 750 000 euros d'amende.
- Usurpation d'identité (article 226-4-1 du code pénal) : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.
- Contrefaçon des marques (logos, signes, emblèmes…) utilisées lors de l'hameçonnage, prévu par les articles L.713-2 et L.713-3 du Code de la propriété intellectuelle. Délit passible d'une peine d'emprisonnement de trois ans et de 300 000 euros d'amende.

pôle emploi

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

PÔLE MÉTAL 2S
Cluster métallurgique

L'ESCROQUERIE AUX **FAUX ORDRES DE VIREMENT (FOVI)**

COMPRENDRE LES RISQUES

L'escroquerie aux faux ordres de virement (**FOVI**) désigne un type d'arnaque qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié. Parfois présenté comme émanant d'un dirigeant et ayant un caractère « urgent et confidentiel », on parle alors « d'arnaque au Président ». Une variante consiste à usurper l'identité d'un fournisseur pour communiquer de nouvelles coordonnées bancaires (changement de RIB) sur lesquelles il faut effectuer un règlement. Une autre variante consiste à usurper l'identité d'un salarié de l'organisation pour demander le changement des coordonnées bancaires où virer son salaire. Le compte bancaire appartenant à l'escroc est souvent situé à l'étranger. Cette catégorie d'escroquerie est généralement réalisée par téléphone et/ou par messages électroniques, voire les deux, et concerne tous les types d'organisation.

BUT RECHERCHÉ

Escroquerie financière en usurpant l'identité d'un dirigeant, d'un fournisseur ou d'un employé visant à faire verser de l'argent sur un compte bancaire détenu par les cybercriminels. Dans certains cas, cette fraude fait suite au piratage et à l'utilisation de la messagerie de la personne ou entité usurpée.

SI VOUS ÊTES VICTIME

IDENTIFIEZ LES VIREMENTS FRAUDULEUX. Identifiez tous les virements exécutés, en instance ou à venir à destination de l'escroc. Informez votre hiérarchie ainsi que le service comptable et demandez le blocage des coordonnées bancaires frauduleuses dans les applications métiers.

DEMANDEZ LA SUSPENSION DU VIREMENT. Si le virement n'est pas encore effectué, contactez immédiatement votre service comptable pour suspendre la demande de virement frauduleuse.

ALERTEZ IMMÉDIATEMENT VOTRE BANQUE ET DEMANDEZ LE RETOUR DES FONDS. Si le virement a été réalisé, contactez au plus vite votre banque pour demander le retour des fonds. Votre dépôt de plainte pourra être exigé de votre banque pour récupérer les sommes.

CONSERVEZ LES PREUVES et en particulier les numéros de téléphones, les messages reçus, les ordres de virement, les factures et toutes informations qui pourront vous servir pour signaler l'escroquerie aux autorités.

SI LA FRAUDE A PU ÊTRE PERMISE PAR LE PIRATAGE D'UN COMPTE DE MESSAGERIE, CHANGEZ IMMÉDIATEMENT SON MOT DE PASSE. Utilisez des mots de passe différents et complexes pour chaque site et application utilisés (tous nos conseils pour gérer vos mots de passe).

DÉPOSEZ PLAINTE. En parallèle des démarches auprès de votre banque, déposez plainte sans tarder au commissariat de police ou à la gendarmerie dont vous dépendez en fournissant toutes les preuves en votre possession.

MESURES PRÉVENTIVES

Sensibilisez vos collaborateurs et cadres aux risques notamment de réception de messages frauduleux d'hameçonnage (*phishing*) visant à leur dérober leurs mots de passe et en particulier si vos services de messagerie sont hébergés ou accessibles en externe.

Diffusez 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.

Mettez en place une procédure de vérification et de validation hiérarchique interne non dérogeable des demandes de virement imprévues ou d'acceptation de changements de coordonnées bancaires.

Veillez à limiter la publication d'informations (site Internet, réseaux sociaux…) permettant d'identifier et de contacter vos collaborateurs habilités à réaliser des demandes de virement ou des modifications de coordonnées bancaires.

Généralisez l'utilisation de mots de passe solides pour les comptes de messagerie et activez la double authentification pour limiter les risques de piratage (tous nos conseils pour gérer vos mots de passe).

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- **Escroquerie (article 313-1 du code pénal).** L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (article 313-3 du code pénal).
- **Usurpation d'identité (article 226-4-1 du code pénal).** Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (article 225-5 du code pénal).
- **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal).** Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. La tentative des délits prévus par les articles 323-1 à 323-3-1 est passible des mêmes peines.

pôle emploi

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

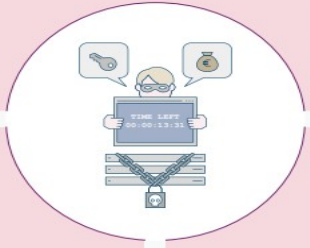
RANÇONGICIEL
Vos données sont prises en otage

QUE SE PASSE-T-IL ?

1. Vos données sont progressivement chiffrées, ce qui les rend inaccessibles

2. L'infection peut s'étendre à tous les appareils connectés au réseau ou aux supports USB branchés

3. On exige de vous le paiement d'une rançon pour récupérer ces données



Impact de l'attaque

Intégrité
Disponibilité
Confidentialité
Authenticité

Motivations principales

Atteinte à l'image
Appât du gain
Revendication
Espionnage
Nuisance

COMMENT RÉAGIR ?
Vous êtes victime d'un rançongiciel
Ne payez pas !

1 - Ne pas éteindre la machine concernée
La mettre en veille prolongée si possible

2 - Déconnectez immédiatement les appareils du réseau

3 - Ne connectez plus aucun appareil sur le réseau

4 - Contactez immédiatement votre service informatique ou un expert (ou trouvez le vôtre sur www.cybermalveillance.gouv.fr)

5 - Portez plainte auprès des services compétents

COMMENT SE PROTÉGER ?
Ne tombez pas dans le piège

Effectuez des sauvegardes régulières de vos données

Mettez à jour régulièrement vos principaux logiciels
- Les rançongiciels utilisent les vulnérabilités des programmes pour se propager

Privilégiez un compte utilisateur pour vos usages courants

Courriers électroniques piégés
- Ne faites pas confiance à l'expéditeur de courriers électroniques dont l'origine ou la forme vous semblent douteuses
- Méfiez-vous des pièces jointes et des liens suspects

En savoir plus sur les attaques par rançongiciel :
www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/
www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Version 2.0 - Janvier 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Alerte aux rançongiciels
Vos données en otage, contre de l'argent !

Vous êtes de plus en plus nombreux à recevoir des messages douteux avec des pièces jointes et/ou des liens qui sont piégés, ***NE CLIQUEZ PAS DESSUS !***

Un virus pourrait chiffrer vos données et exiger une rançon. La payer ne garantit pas la récupération de l'intégralité de vos données.

Il est constaté de plus en plus d'**escroqueries** par des emails qui contiennent des pièces jointes et/ou des liens piégés. **Ces messages frauduleux sont maintenant plus difficiles à détecter** par les utilisateurs car ils sont bien souvent de parfaites copies, avec de vrais logos et sans faute d'orthographe.

VOICI QUELQUES RÈGLES DE BON SENS QU'IL FAUT ABSOLUMENT RESPECTER :

Ces réflexes sont indispensables et peuvent sauver votre entreprise !

N'ouvrez pas les messages dont la provenance ou la forme est douteuse.
Apprenez à distinguer des emails piégés en deux minutes sur :
https://www.hack-academy.fr/candidats/willy

Effectuez des sauvegardes régulières de vos données.
Déplacez physiquement la sauvegarde de votre réseau et placez-la en lieu sûr.
Assurez-vous aussi qu'elle fonctionne.

Mettez à jour vos principaux outils : Windows, antivirus, lecteur PDF, navigateur, etc.
Et si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera la propagation des rançongiciels via les vulnérabilités des applications.

Créer un compte « utilisateur » et n'utilisez que celui-ci, une fois votre ordinateur configuré.
Cette règle ralentira l'escroc dans ses actions malveillantes.

Vous trouverez toutes les recommandations de l'ANSSI sur le site :
http://ssi.gouv.fr
En complément, il est recommandé de prendre quotidiennement connaissance des bulletins d'alerte du CERT-FR :
http://www.cert.ssi.gouv.fr
Si besoin, n'hésitez pas à solliciter vos prestataires informatiques sur ces sujets.

FEDERATION EBEN
ENTREPRISES DU BUREAU ET DU NUMÉRIQUE

V12 - 20103518

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

IT

Le cyber « bon-sens » technique et humain

- Mise à jour
- Mots de passe
- Les accès
- Les sauvegardes

Gendarmerie nationale

pôle emploi

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

LES COMPTES

Combien de personnes disposent du mot de passe administrateur permettant d'accéder au système central de gestion des droits ?

Combien de temps se passe-t-il entre le moment où quelqu'un quitte votre organisation et le moment où son compte est supprimé ?

Combien avez-vous de comptes non individuels, de comptes de service ?

Quand, pour la dernière fois, quelqu'un a-t-il vérifié qui disposait des droits d'accès à la messagerie de votre PDG ou DG ?

Quel mot de passe est utilisé pour installer une imprimante ? Le mot de passe permettant le contrôle total de votre système d'information, ou un autre ?

Combien d'accès internet avez-vous ? Où sont-ils ? Sont-ils tous administrés ? Surveillés ?

Qui a vérifié si pendant les vacances, un fichier zip de 2 Go n'avait pas été extrait de votre système d'information ? Quelqu'un regarde-t-il de temps en temps si les flux sortant de votre SI, la nuit par exemple, sont légitimes ? Si les adresses de destination sont normales ? La dernière fois que vous êtes venus travailler un dimanche, quelqu'un est-il venu vous demander le lundi s'il était normal que quelqu'un se soit connecté sur votre compte dimanche ?

Gendarmerie nationale

pôle emploi

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

LES SAUVEGARDES

Contrôler et tester les sauvegardes

Règle des 3-2-1 :

- Créez 3 copies de vos données (1 copie principale et 2 sauvegardes)
- Stockez vos copies sur au moins 2 types de support de stockage (disque local, partage réseau/NAS, lecteur de bandes, etc.)
- Stockez l'une de ces copies hors site (dans le cloud)

Gendarmerie nationale

pôle emploi

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

Gendarmerie nationale

pôle emploi

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

PIRATAGE D'UN SYSTÈME INFORMATIQUE

Pro

COMPRENDRE LES RISQUES

Un système informatique (ou système d'information) désigne tout appareil, équipement ou ensemble de ces matériels, permettant de traiter et stocker des données (ordinateur, appareil mobile, objet connecté, serveur, réseau...). Le piratage d'un système informatique se définit comme l'accès non autorisé à ce système par un tiers. En pratique, les pirates peuvent s'introduire dans un système informatique par l'utilisation d'une faille de sécurité ou d'un défaut de configuration d'un équipement ; l'infection par un logiciel malveillant (virus) ; le vol d'identifiants de connexion suite à un appel ou un message frauduleux (hameçonnage) ; etc. L'origine de l'intrusion peut être interne (collaborateur, prestataire) ou externe (cybercriminels). Une fois introduits, les cybercriminels peuvent chercher à se propager aux autres équipements du réseau attaqué. Une intrusion peut entraîner le vol, voire la destruction, des informations du système touché.

BUT RECHERCHÉ

Prendre le contrôle ou utiliser les ressources d'un équipement pour en faire un usage frauduleux : gain d'argent, espionnage, sabotage, revendication, chantage ou vandalisme.

SI VOUS ÊTES VICTIME

METTEZ EN QUARANTAINE LES ÉQUIPEMENTS concernés par l'incident.

IDENTIFIEZ LA SOURCE DE L'INTRUSION (faille de sécurité, message malveillant...) pour la corriger.

IDENTIFIEZ TOUTE ACTIVITÉ INHABITUELLE : création de comptes, ajout de fichier dans le système, etc.

ÉVALUEZ L'ÉTENDUE DE L'INTRUSION à d'autres appareils ou équipements.

COLLECTEZ LES PREUVES : journaux (logs) des pare-feu et serveurs, copie complète (physique) des équipements compromis et de leur mémoire...

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie dont vous dépendez avec toutes les preuves en votre possession.

RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE de l'ensemble de vos équipements.

RÉINSTALLEZ LE SYSTÈME compromis depuis une sauvegarde antérieure à l'attaque.

CHANGEZ LES MOTS DE PASSE d'accès aux équipements touchés.

METTEZ À JOUR LES LOGICIELS ET ÉQUIPEMENTS avant la remise en service de votre système.

NOTIFIEZ L'INTRUSION À LA CNIL en cas de violation de données à caractère personnel.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS SPÉCIALISÉS que vous pourrez trouver sur www.cybermalveillance.gouv.fr.

MESURES PRÉVENTIVES

Utilisez, paramétrez et mettez à jour régulièrement votre antivirus et les équipements de sécurité de votre système informatique (pare-feu, etc.).

Mettez à jour régulièrement les appareils, les systèmes d'exploitation ainsi que les logiciels installés de vos équipements.

N'installez pas de logiciels, programmes, applications ou équipements « piratés » ou dont l'origine ou la réputation est douteuse.

N'utilisez les comptes administrateurs qu'en cas de nécessité.

Limitez les privilèges et les droits des utilisateurs au strict nécessaire.

Vérifiez régulièrement les fichiers de journalisation de vos équipements afin d'identifier toute activité inhabituelle.

Utilisez des mots de passe suffisamment complexes et changez-les au moindre doute (tous nos conseils pour gérer vos mots de passe).

Faites des sauvegardes régulières et déconnectées de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens provenant d'expéditeurs inconnus ou dont le contenu est inhabituel.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

PÔLE MÉTAL 2S
Cluster métallurgique

LES INFRACTIONS

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- L'infraction d'**atteinte à un système de traitement automatisé de données (STAD)** peut être retenue. Les articles 323-1 à 323-7 du code pénal disposent que : « *le fait d'accéder ou de se maintenir frauduleusement* » dans un STAD, « *la suppression ou la modification de données contenues dans le système* », ou l' « *altération du fonctionnement de ce système* » sont passibles de deux ans à sept ans d'emprisonnement et de 60 000 euros à 300 000 euros d'amende.
- **La tentative de cette infraction est également punissable** (article 323-7 du Code pénal) : « *La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines* ».

pôle emploi

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

LIENS UTILES

- cyber-vigilance-nouvelleaquitaine@gendarmerie.interieur.gouv.fr
- securite-economique-nouvelleaquitaine@gendarmerie.interieur.gouv.fr
- https://www.ssi.gouv.fr/
- https://www.cybermalveillance.gouv.fr/
- https://www.gendarmerie.interieur.gouv.fr/a-votre-contact/contacter-la-gendarmerie/discuter-avec-un-gendarme-de-la-brigade-numerique
- https://www.signal-spam.fr
- https://phishing-initiative.fr/contrib/
- https://signal.conso.gouv.fr/

Gendarmerie nationale

pôle emploi

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

CLUSIF

https://clusif.fr/publications/guide-cybersecurite-des-systemes-industriels-2021/

- cartographie des systèmes industriels ;
- appréciation des risques cyber ;
- architecture sécurisée ;
- intégration et recette de sécurité ;
- maintien en conditions de sécurité.

Gendarmerie nationale

pôle emploi

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

LES GUIDES ANSSI

https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-treize-questions/

Gendarmerie nationale

pôle emploi

Cybermenaces et Covid-19

Recommandations pour les entreprises et les salariés en télétravail

Faux sites liés au COVID19

• Prenez garde aux faux sites Internet relatifs aux ventes en ligne de masques, gel hydroalcoolique.

Fausses commandes et faux ordre de virement

• Vérifiez la signature de documents ou les tentatives de récupération des mots de passe de vos données d'entreprise.

• Vérifiez les demandes d'un virement exceptionnel ou un changement de RIB d'une facture ou d'un salaire faite par un dirigeant, d'un fournisseur, d'un prestataire, voire d'un collaborateur, pour demander un virement exceptionnel ou un changement de RIB d'une facture ou d'un salaire. Son identité a pu être usurpée suite au piratage d'un compte de messagerie, par message et même téléphone.

L'hameçonnage / Phishing

• méfiez-vous des mails, SMS, chat (réseaux sociaux, messageries instantanées type Whatsapp) et appels téléphoniques non identifiés. Cette technique soustrait des informations personnelles, professionnelles ou bancaires en vous orientant sur de faux sites.

Portails d'information

www.contacterlagendarmerie.fr
www.cybermalveillance.gouv.fr
www.ssi.gouv.fr
www.cnil.fr

Dons frauduleux

• Évitez de cliquer sur les liens des appels aux dons et rendez vous directement sur le site officiel.

Rançongiciel / Ransomware

Cette attaque consiste à empêcher l'accès aux données de l'entreprise et à réclamer une rançon pour les libérer. Elle s'accompagne d'un vol de données et d'une destruction préalable des sauvegardes.

Elles sont possibles par une intrusion sur le réseau de l'entreprise, un accès à distance, par la compromission de l'équipement d'un collaborateur ou un défaut de mise à jour du matériel informatique (pièces jointes ou liens présents dans les courriers électroniques).

Pensez à :

Bilan sécurité et sauvegarde des données

• Profitez du ralentissement de l'activité, faites un bilan complet avec votre responsable informatique ou une entreprise cybersécurité.

• Procédez à des sauvegardes régulières et hors ligne des données. Déconnectez votre support de sauvegarde à l'issue.

Attestation de travail

• Facilitez la mobilité de vos salariés en éditant des attestations de déplacement dérogatoire avec le timbre officiel de l'entreprise.

Déplacements / Télétravail

• Vos collaborateurs et salariés doivent renforcer leur vigilance lors de leurs trajets domicile/lieu de travail, en particulier leurs équipements mobiles.

• Mettez à disposition des solutions de sécurité (VPN, antivirus) et assurez-vous qu'ils connaissent les règles de mise en œuvre et de mise à jour.

• Proscrivez à vos collaborateurs l'emploi d'espaces de partage personnel des documents.

• Rappelez les consignes et contacts en cas d'incident.

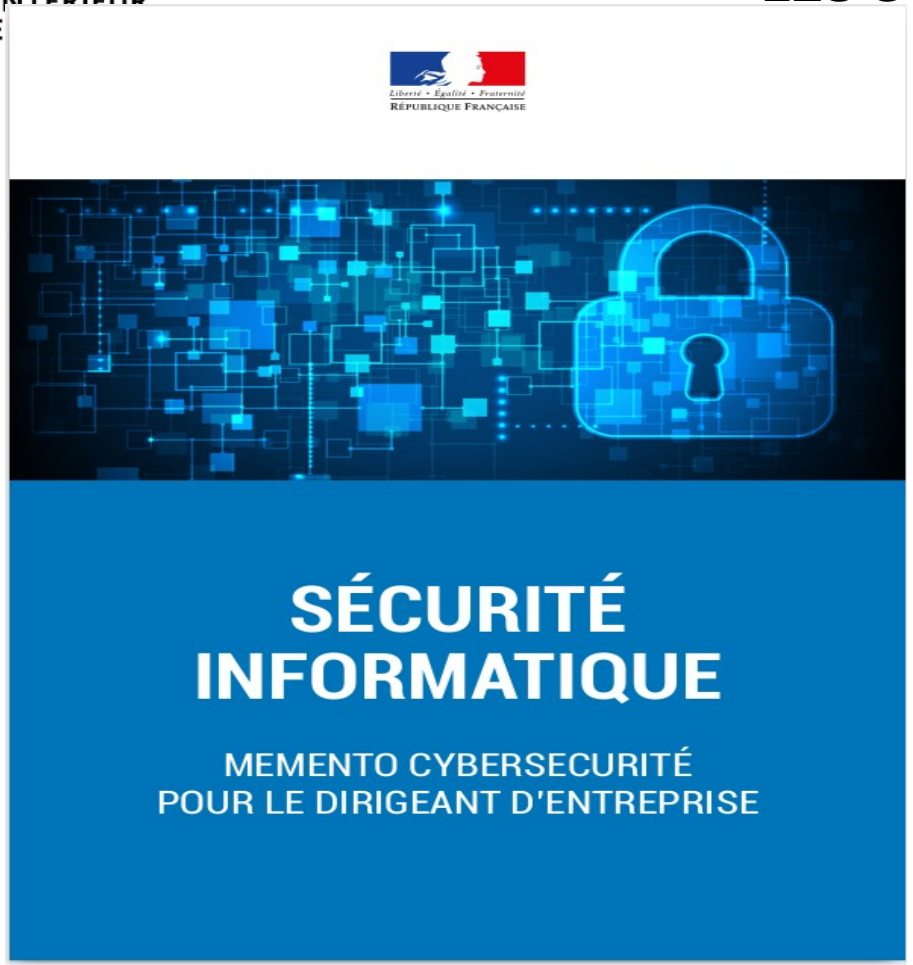
Charte informatique

• Faites un rappel sur les droits et devoirs de chacun sur les règles d'utilisation du réseau informatique de l'entreprise.

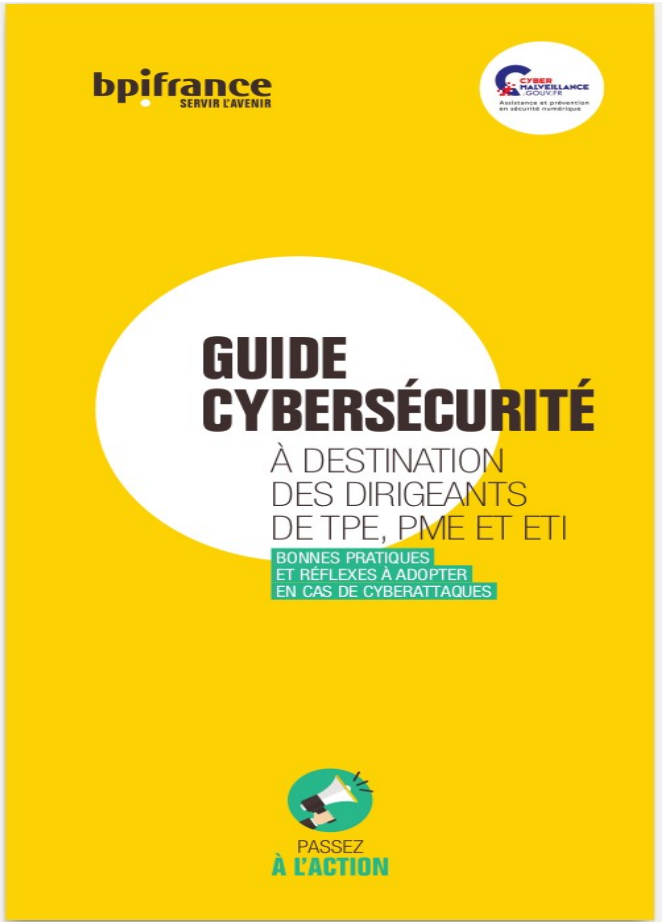
• Si nécessaire, mettez à jour les consignes et les nouveaux outils du travail à distance.

Conception graphique Sirpa-gendarmerie C 8889 - 2020

LES GUIDES ANSSI



https://www.economie.gouv.fr/files/files/PDF/2017/bro-memento-cybersecurite-createur_0.pdf

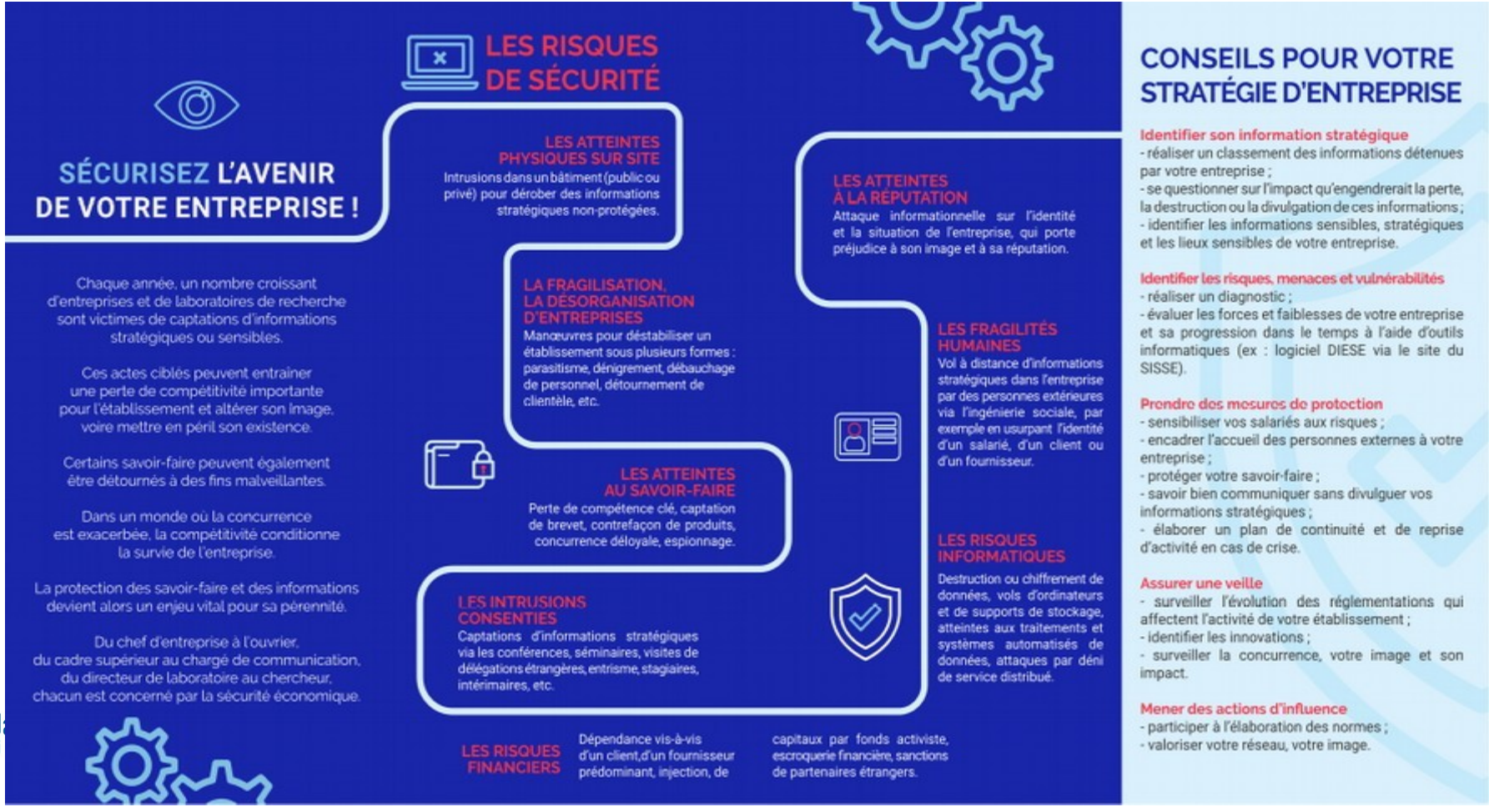


https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillancegouvfr-bpifrance-guide-pme-tpe

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

PÔLE MÉTAL2S
Cluster métallurgique



Gend
nati

pôle emploi

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

PÔLE MÉTAL 2S
Cluster métallurgique

LES ACTEURS

VOUS SOUHAITEZ SÉCURISER VOS MARCHÉS ET VOTRE SAVOIR-FAIRE EN FRANCE ET À L'INTERNATIONAL ?

LA DIRECTION GÉNÉRALE DES DOUANES

- prévient les pratiques agressives et déloyales ;
- préserve les intérêts français à l'étranger via son réseau international d'attachés douaniers ;
- participe au contrôle des investissements étrangers en France ;
- promeut l'agrément Opérateur Economique Agréé (OEA), label de confiance douanier européen.

Contact
+33 (0) 9 70 27 55 80
pae-bordeaux@douane.finances.gouv.fr
Outil
www.douane.gouv.fr

L'ASSOCIATION FRANÇAISE DE NORMALISATION (AFNOR)

- propose des solutions fondées sur les normes volontaires, documents consensuels reflétant les bonnes pratiques les plus reconnues au niveau européen et international.

Contact
+33 (0) 5 57 29 14 33
delegation.bordeaux@afnor.org
Outil
https://normalisation.afnor.org/thematiques/numerique/

L'INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE (INPI)

- accompagne les entreprises, sur le territoire et à l'export, en matière de propriété industrielle pour protéger le savoir-faire des acteurs économiques en France.

Contact
0820 210 211
nouvelleaquitaine@inpi.fr
Outil
www.inpi.fr

VOUS SOUHAITEZ PROTÉGER VOS INFORMATIONS STRATÉGIQUES, VOS LOCAUX, SENSIBILISER VOS SALARIÉS, FAIRE UN DIAGNOSTIC ?

LA DIRECTION ZONALE DE SÉCURITÉ INTÉRIEURE (DZSI)

- participe à la protection du patrimoine scientifique et technique de la nation (PPST) ;
- apporte son expertise en matière de sécurité économique ;
- accompagne les entreprises dans leurs démarches de protection des informations stratégiques et sensibles.

Contact
securite-economique-bordeaux@interieur.gouv.fr
Outil
La lettre d'information « Flash Ingérence » disponible sur abonnement, à solliciter par écrit à l'adresse ci-dessus.

L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

- apporte son expertise et son assistance technique aux administrations et aux entreprises dans leur développement numérique ;
- assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

Contact
nouvelle-aquitaine@ssi.gouv.fr
Outils
www.ssi.gouv.fr
https://secnumacademie.gouv.fr/ (formation à distance)

LES DÉLÉGUÉS À L'INFORMATION STRATÉGIQUE ET À LA SÉCURITÉ ÉCONOMIQUES (DISSE)

- informent, orientent et conseillent les acteurs économiques en matière de sécurité économique.

Contact
na.disse@direccte.gouv.fr
Outils
Guide des 26 fiches de sécurité économique et DIESE (diagnostic d'intelligence économique et de sécurité économique) sur : https://sisse.entreprises.gouv.fr

GENDARMERIE : LES RÉFÉRENTS SÉCURITÉ ÉCONOMIQUE ET PROTECTION DES ENTREPRISES (SÉcoPE)

- aident à l'identification des risques et à l'adaption des dispositifs de protection ;
- organisent des actions de sensibilisation et de prévention au profit de différents acteurs (entreprises, associations, facultés...).

Contact
securite-economique-nouvelleaquitaine@gendarmerie.interieur.gouv.fr
Outil
Jeu des 8 familles d'atteintes à la sécurité économique sur **www.gendarmerie.interieur.gouv.fr**

LE SERVICE ZONAL DU RENSEIGNEMENT TERRITORIAL (SZRT 33)

- assure le suivi économique et social des entreprises dans les départements ;
- exerce des fonctions de capteur dans la mise en œuvre globale de la politique publique d'intelligence économique ;
- détecte les vulnérabilités et les atteintes aux entreprises.

LA DÉLÉGATION RÉGIONALE À LA RECHERCHE ET À LA TECHNOLOGIE (DRRT)

- participe à la sensibilisation des établissements d'enseignement supérieur, des organismes publics et privés de recherche, des centres de ressources technologiques (CRT) ainsi que des jeunes entreprises innovantes (JEI), en matière de sécurité économique.

Contact
drrt.nouvelle-aquitaine@recherche.gouv.fr

VOUS ÊTES UNE ENTREPRISE ACTIVE SUR LES MARCHÉS DÉFENSE, OU INTÉRESSÉE PAR CES OPPORTUNITÉS ?

LA DIRECTION DU RENSEIGNEMENT ET DE LA SÉCURITÉ DE LA DÉFENSE (DRSD)

- décèle et neutralise toute menace contre les intérêts nationaux et la souveraineté nationale, touchant la sphère défense ;
- assure le suivi, la sensibilisation, le conseil des industries et instituts de formation ou de recherche en lien avec la défense dans sa mission de contre-ingérence économique (incluant la cyber défense).

Contact
+33 (0) 5 57 85 10 22
drsd-bordeaux-cie.contact.fct@intradef.gouv.fr
Outils
www.drsd.defense.gouv.fr

LA DIRECTION GÉNÉRALE DE L'ARMEMENT (DGA)

- accompagne les PME de la base industrielle et technologique de défense (BITD) dans leur projet de développement (innovation, exportation, accès au marché) ;
- contribue à la sensibilisation des PME et ETI à la sécurité économique et à la cybersécurité.

Outils
www.achats.defense.gouv.fr (espace PME)
www.ixarm.com

SISSE
www.prefectures-regions.gouv.fr/nouvelle-aquitaine
@PrefAquitaine33 @PrefetNouvelleAquitaine33

ENTREPRISES ET LABORATOIRES
EN NOUVELLE-AQUITAINE

PROTÉGEZ VOS INFORMATIONS STRATÉGIQUES

Liberté
Égalité
Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET
DE LA RÉGION
NOUVELLE-AQUITAINE

loi

#RÉPONDREPRÉSENT

GENDARMERIE
NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

Opération tranquillité Entreprise et Commerce

La gendarmerie peut surveiller votre commerce, entreprise ou son périmètre
Signalez vous auprès de votre brigade pour en bénéficier

FERMETURE EXCEPTIONNELLE COVID 19

Votre commerce/ entreprise est fermé

- **Fermez** bien tous les accès de votre commerce ou entreprise.
- Dans la mesure du possible, limitez les stocks et **ne conservez pas** d'argent liquide.
- **Activez** vos systèmes de protection : éclairage, alarme, vidéo. Vérifiez régulièrement leur bon fonctionnement.
- En l'absence de client et d'employé **vous pouvez installer** un dispositif de vidéosurveillance sans formalité particulière.

OUVERT

Votre commerce/ entreprise est ouvert

- **Soyez attentif à votre environnement,** détectez les comportements inhabituels et signalez-les nous.
- **Vérifiez régulièrement le bon fonctionnement** de vos équipements de protection déjà en place : éclairage, système d'alarme et vidéo le cas échéant.
- Si possible, ouvrez et quittez à plusieurs les locaux.
- **Ne stockez pas** vos produits à la vue des clients.
- **Limitez, si possible,** les stocks de produits de grande valeur.
- **Rappelez** à vos collaborateurs et/ou employés les mesures élémentaires de sûreté (fermetures effectives des ouvrants, activation des alarmes…).

Prévention Cyber

Plus de conseils sur www.cybermalveillance.gouv.fr

- Attention aux cyberattaques, aux escroqueries ou aux démarchages directs, notamment si vous fonctionnez en télétravail : ne relâchez pas votre vigilance et sensibilisez vos collaborateurs !
- Maîtrisez la communication de vos activités et l'utilisation des réseaux sociaux pour ne pas susciter l'intérêt d'un délinquant.

Vous êtes victime

#RÉPONDREPRÉSENT

- **En cas d'urgence,** appelez le 17 ou 112
- **En cas de cambriolage,** ne touchez à rien et composez le 17
- Pour les vols, dégradations, escroqueries : **www.pre-plainte-en-ligne.gouv.fr**
- Votre sûreté a des vulnérabilités fortes, les référents et correspondants sûreté de la gendarmerie peuvent vous conseiller. **Adressez-vous** à votre brigade de gendarmerie : **www.interieur.gouv.fr/Contact/Contacter-une-brigade-de-gendarmerie-ou-un-commissariat-de-police**

Conception graphique Sirpa-gendarmerie C 891 - 2020