assure
MAÎTRISONS NOS ÉNERGIES

Rencontre thématique du programme assURE

LACROIX
CONNECTED TECHNOLOGIES
FOR A SMARTER WORLD

PRESENTATION – Gildas Rémois

CYBERSECURITE
Appliquée au monitoring GTC/GTB

Sommaire

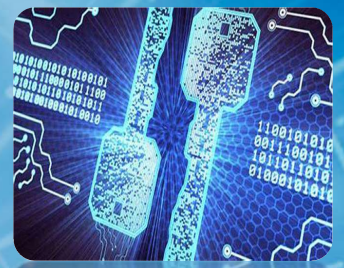
LACROIX

Qu’est-ce que la Cybersécurité

- C’est un ensemble de technologies, de processus et de pratiques conçus pour gérer le risque du cyberespace.
- La cybersécurité cherche à garantir la sécurité des données de façon globale

Pourquoi la cybersécurité sur un réseau industriel?

- L’automatisation, la communication ou la gestion à distance sont indispensables pour le contrôle efficace des installations.
- La sécurité est essentielle pour protéger les installations et garantir un fonctionnement permanent.



L'intégration de **la cybersécurité** dans l'environnement numérique est essentielle pour une évolution optimale et sûre.

La cybersécurité doit relever **4 enjeux majeurs.**

CONFIDENTIALITÉ

Garantir la confidentialité des données en chiffrant les échanges de données pour éviter leur utilisation par des tiers malveillants.

INTEGRITÉ

S'assurer que les informations n'ont pas été modifiées intentionnellement ou non.

AUTHENTIFICATION

Garantie de l'identité de l'intervenant : fournir une preuve d'origine dans le message.

TRACABILITÉ

Suivre toutes les actions dans les journaux (alarme, connexion, modification de la configuration) afin de suivre les actions des utilisateurs.

Pourquoi la Cyber sur un réseau technique?

Types de menaces

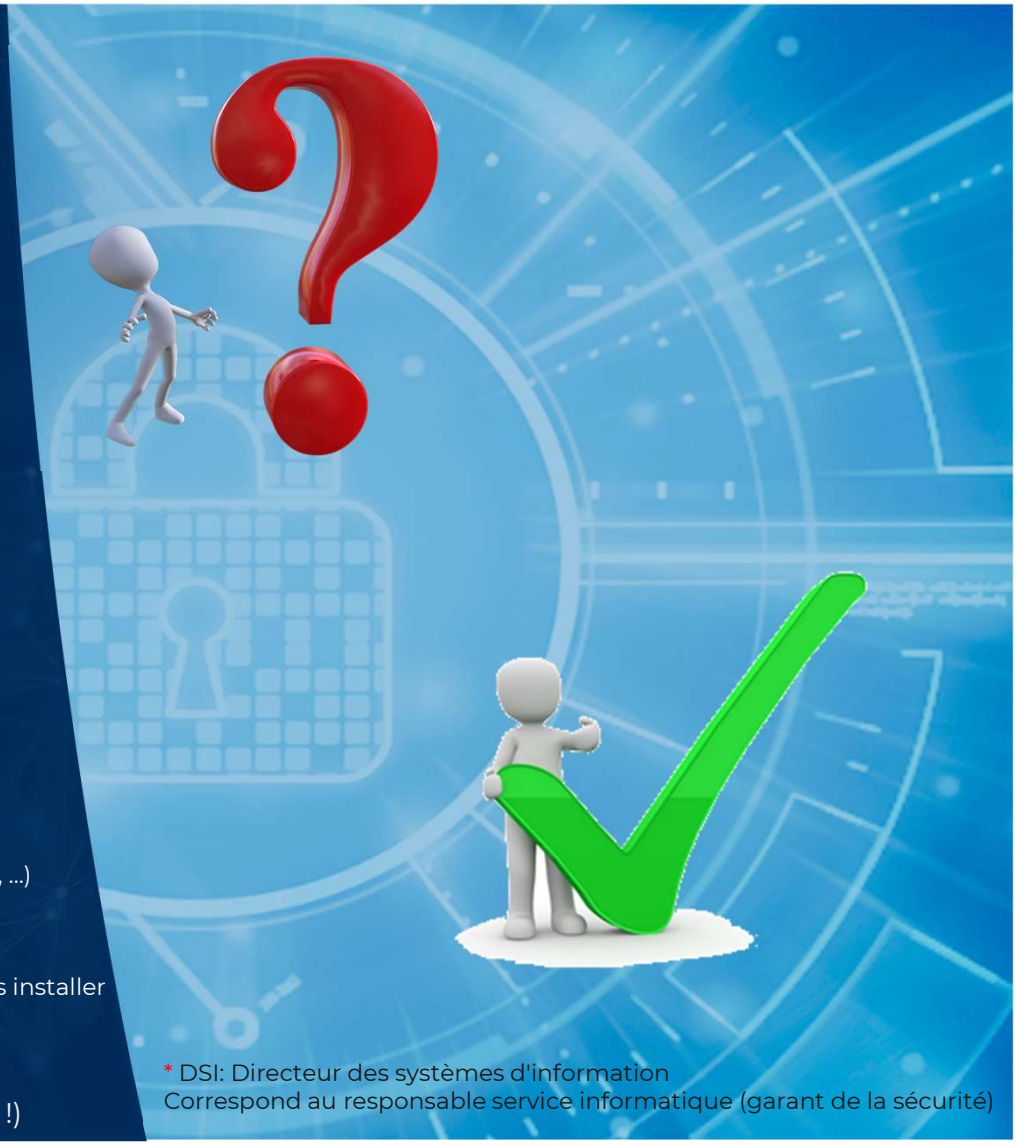
- Mauvaise manipulation
- Employé en désaccord avec l'entreprise
- Intrusion sur le réseau
- Ransomware

Types de risques

- Compromettre une installation
- Indisponibilité
- Vol d'information
- Perte financière

Types d'action à mettre en œuvre

- Réseau (A la charge du DSI *)
  - Retarder/ Décourager l'attaquant par la mise en place de différents mécanismes
  - Être alerté au plus vite d'un dysfonctionnement
  - Disposer de journaux de suivi pour retracer les évènements
- Postes utilisateurs (A la charge de la DSI *)
  - Limiter les niveaux d'accès aux seuls personnes habilités
  - Limiter les actions en fonction des profils
  - Pouvoir limiter à distance les niveaux de droits
- Automate (A la charge de la cellule production)
  - Limiter les niveaux d'accès aux seuls personnes habilités (MAJ programme, forçage, ...)
  - Pouvoir limiter à distance les niveaux de droits
  - Traçabilité des actions et des connexions
  - Firmware signé numériquement par le constructeur
  - Se tenir informé des MAJ de sécurité mises à disposition par les constructeurs, et les installer
  - Impossibilité d'utiliser l'automate comme point de rebond
  - Garant de l'intégrité des informations transmises
- Dissocier les usages Personnels et Professionnels (A la charge de Chacun !)



* DSI: Directeur des systèmes d'information
Correspond au responsable service informatique (garant de la sécurité)

Exemple de cybers attaques

2010: 1ere cyber attaque à faire les gros titres dans le monde visant le programme nucléaire Iranien

30.000 ordinateurs infectés par le virus Stuxnet, spécialement conçu pour attaquer les systèmes informatiques industriels (Siemens Wincc) Lien

2016: Mise hors service partielle d'une centrale électrique en Ukraine

Intervention de personnes non autorisées (...) dans le système de commande à distance" les techniciens avaient alors dû rétablir le courant "manuellement " (...)
75 minutes pour rétablir le courant en plein mois de décembre avec des températures extérieures négatives Lien / Lien

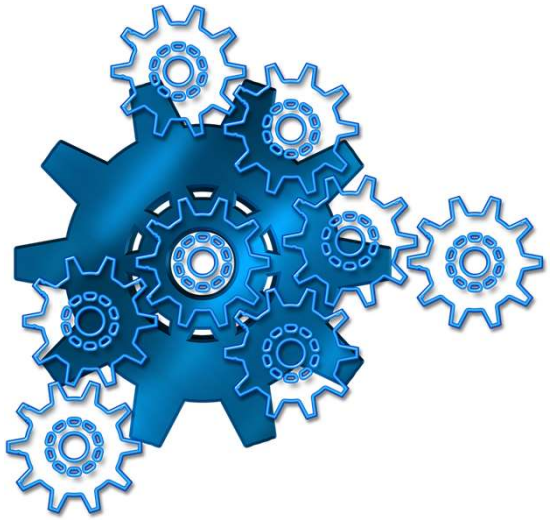
2018: Un casino piraté à cause d'un thermomètre connecté dans un aquarium

Les attaquants s'en sont servis pour mettre un pied dans le réseau, puis ils ont trouvé la base de données client Lien

2022: 6000 éoliennes allemandes touchées par une cyberattaque russe

Attaque sur des infrastructures de communications satellites (Viasat) impactant environ 30.000 clients internet, parmi eux environ 6000 eoliennes du fabricant allemand Enercon Lien

Et beaucoup d'autres touchant aussi bien les professionnels que les particuliers ...



De Facon Globale, il est nécessaire de connaitre son réseau et savoir agir en cas d'attaques, deux possibilités

PCA : le plan de continuité d'activité

L'ambition du PCA est de garantir la disponibilité du SI de l'entreprise en cas d'attaque.

Autrement dit, le PCA garantit que toutes les applications critiques restent en état d'activité et que toutes les données sont conservées afin que les collaborateurs puissent tous poursuivre leur activité.

D'un point de vue technique, le PCA prévoit essentiellement des **redondances d'installations,** de serveurs, de machines et de logiciels, afin que ces géantes roues de secours prennent le relais le plus vite possible en cas de nécessité.

PRA : le plan de reprise d'activité

Mettre en place un PCA est un vaste projet, parfois très long et très coûteux

Sans PCA, le PRA intervient en dernier lieu, il expose toutes les procédures à suivre en cas de défaillance de l'informatique et des systèmes d'information.

L'idée est de suivre les étapes nécessaires pour **restaurer une globalité d'applications et de machines** telles qu'elles étaient avant l'incident technique, **sans pertes** d'informations, le plus souvent à partir d'une infrastructure et de données de secours – à jour, bien évidemment.

Source: https://www.wandesk.fr/

Solutions réseaux:
Utilisation de firewalls, serveurs VPN, routeurs,

- Filtre les flux autorisés (http, https, FTP, ..)
- Adresses autorisées
- Réseaux virtuels (VLAN)
- Surveille les flux et les paquets de données

- La mise en place des différents mécanismes permet de retarder/ décourager l'attaquant
- Mise en route et **maintien en état opérationnel complexe.**
- Nécessite de fortes compétences informatiques pour assurer les communications en fonctionnement normal

Solutions informatiques:
Certificats électroniques et protocoles de sécurisés

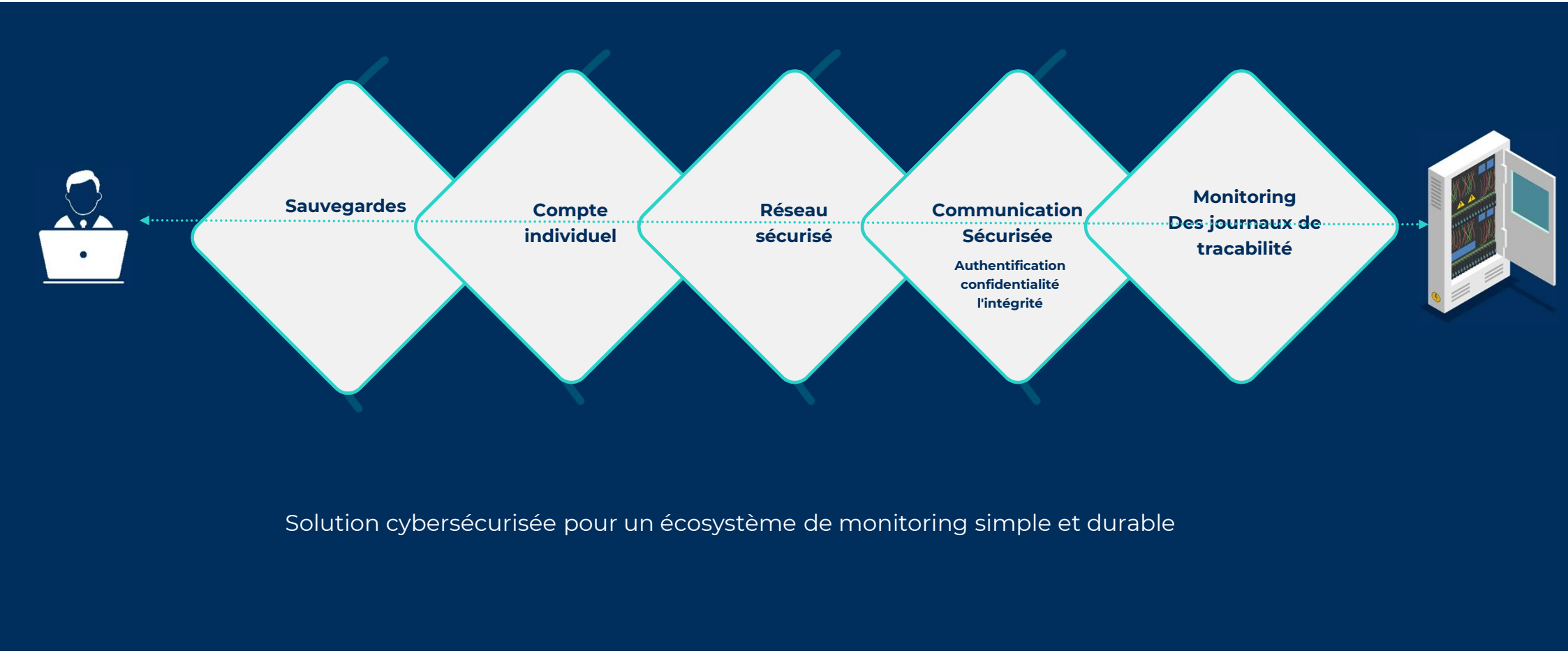
- Répondre à l'authenticité
- Répondre à la confidentialité et l'intégrité
- Transparent pour l'utilisateur

- Mise en œuvre relativement simple par le déploiement d'une autorité de confiance, pour la gestion des certificats
- Souplesse et simplicité de renouvellement des certificats de façon automatique garantissant la sécurité de bout en bout,
- Les **Protocoles de sécurités** doivent êtres **implémentés nativement** dans les produits **par les fabricants/développeurs** et être simple à mettre en oeuvre
- Une architecture réseau sécurisée reste indispensable

Microsoft

Autorité de certification: PKI

Bonnes pratiques en matière de cybersécurité rapporté à une solution de monitoring GTC/GTB



Solution cybersécurisée pour un écosystème de monitoring simple et durable

Création de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) en 2009

- Service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN),
- l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique.
- Acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV).
- Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

L'ANSSI peut délivrer deux type de visas de sécurité

- Un certification attestant de la robustesse d'un produit,
- Une qualification, recommandation par l'État français de produits ou services de cybersécurité éprouvés et approuvés.

La qualification que délivre l'ANSSI vous permet d'identifier facilement les solutions de cybersécurité les plus fiables

Pour aller plus Loin:

Ce Guide s'adresse aux entités publiques ou privées pour leurs permettre de veiller à leur sécurité.

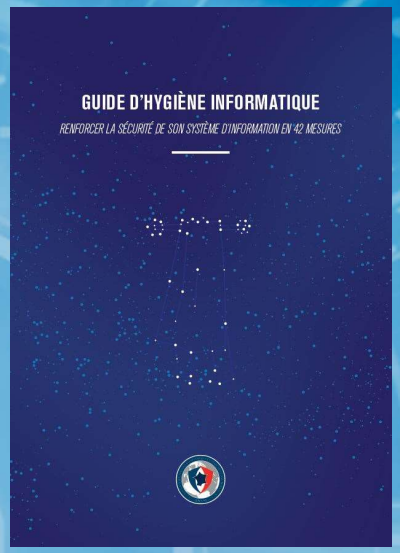
Il est né du constat que si les mesures qui y sont édictées avaient été appliquées par les entités concernées, la majeure partie des attaques informatiques ayant requis une intervention de l'ANSSI aurait pu être évitée.

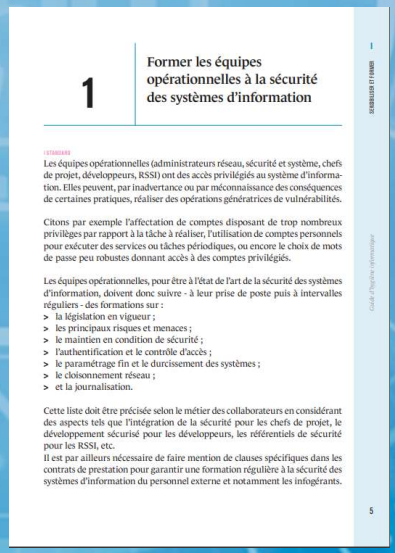
La sécurité n'est plus une option.

À ce titre, les enjeux de sécurité numérique doivent se rapprocher des préoccupations économiques, stratégiques ou encore d'image qui sont celles des décideurs.

ce guide d'hygiène informatique est une feuille de route qui épouse les intérêts de toute entité consciente de la valeur de ses données

Disponible gratuitement: https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/





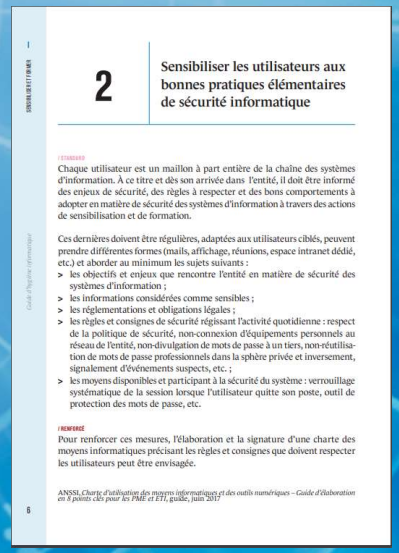
1 Former les équipes opérationnelles à la sécurité des systèmes d'information

Les équipes opérationnelles (administrateurs réseau, sécurité et système, chefs de projet, développeurs, RSSI) ont des accès privilégiés au système d'information. Elles peuvent, par inadvertance ou par méconnaissance des conséquences de certaines pratiques, réaliser des opérations génératrices de vulnérabilités.

Citons par exemple l'affectation de comptes disposant de trop nombreux privilèges par rapport à la tâche à réaliser, l'utilisation de comptes personnels pour exécuter des services ou tâches périodiques, ou encore le choix de mots de passe peu robustes donnant accès à des comptes privilégiés.

Les équipes opérationnelles, pour être à l'état de l'art de la sécurité des systèmes d'information, doivent donc suivre - à leur prise de poste puis à intervalles réguliers - des formations sur :
- la législation en vigueur ;
- les principaux risques et menaces ;
- le maintien en condition de sécurité ;
- l'authentification et le contrôle d'accès ;
- le paramétrage fin et le durcissement des systèmes ;
- le cloisonnement réseau ;
- et la journalisation.

Cette liste doit être précisée selon le métier des collaborateurs en considérant des aspects tels que l'intégration de la sécurité pour les chefs de projet, le développement sécurisé pour les développeurs, les référentiels de sécurité pour les RSSI, etc.
Il est par ailleurs nécessaire de faire mention de clauses spécifiques dans les contrats de prestation pour garantir une formation régulière à la sécurité des systèmes d'information du personnel externe et notamment les infogérants.



2 Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique

Chaque utilisateur est un maillon à part entière de la chaîne des systèmes d'information. À ce titre et dès son arrivée dans l'entité, il doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des systèmes d'information à travers des actions de sensibilisation et de formation.

Ces dernières doivent être régulières, adaptées aux utilisateurs ciblés, peuvent prendre différentes formes (mails, affichage, réunions, espace intranet dédié, etc.) et aborder au minimum les sujets suivants :
- les objectifs et enjeux que rencontre l'entité en matière de sécurité des systèmes d'information ;
- les informations considérées comme sensibles ;
- les réglementations et obligations légales ;
- les règles et consignes de sécurité régissant l'activité quotidienne : respect de la politique de sécurité, non-connexion d'équipements personnels au réseau de l'entité, non-divulgation de mots de passe à un tiers, non-réutilisation de mots de passe professionnels dans la sphère privée et inversement, signalement d'événements suspects, etc. ;
- les moyens disponibles et participant à la sécurité du système : verrouillage systématique de la session lorsque l'utilisateur quitte son poste, outil de protection des mots de passe, etc.

Pour renforcer ces mesures, l'élaboration et la signature d'une charte des moyens informatiques précisant les règles et consignes que doivent respecter les utilisateurs peut être envisagée.

ANSSI, *Charte d'utilisation des moyens informatiques et des outils numériques – Guide d'élaboration en 8 points clés pour les PME et ETI*, guide, juin 2017

Merci

Suivez-nous sur les réseaux sociaux