Dans le cadre de ma formation en BTS SIO option SISR, j'ai réalisé une veille technologique ayant pour sujet la cybersécurité au sein des PME.

J'ai choisi ce thème car, ayant pour objectif de créer ma propre société, cela me permet de mieux comprendre les risques ainsi que les solutions à mettre en place lors de la création de mon entreprise.

La cybersécurité est un enjeu majeur pour les PME, car une attaque peut entraîner des conséquences graves, allant de l'arrêt total de l'activité jusqu'à la perte de données. De plus, les PME disposent généralement de moins de moyens humains et financiers pour se protéger efficacement.

Au cours de mes recherches, plusieurs types d'attaques sont revenus à de nombreuses reprises :

- Les ransomwares : ils représentent aujourd'hui l'une des principales menaces. Ils chiffrent les données de l'entreprise et exigent une rançon en échange de leur restitution. Les PME sont particulièrement visées car elles sont souvent moins sécurisées.
- Le phishing : il consiste à tromper un employé afin d'obtenir des identifiants ou d'introduire un malware dans le système informatique.
- L'exploitation de vulnérabilités : de nombreuses attaques exploitent des failles connues sur des serveurs, VPN, pare-feu ou CMS non mis à jour.
- Les mauvaises configurations réseau : ports ouverts inutilement, absence de segmentation réseau, mots de passe faibles ou identiques sur plusieurs services.

Pour contrer ces menaces, j'ai identifié plusieurs solutions et bonnes pratiques :

- Les sauvegardes selon la règle 3-2-1 : cela correspond à 3 copies des données, sur 2 supports différents, dont 1 sauvegarde externalisée.
- La mise en place du MFA : il s'agit d'une authentification multi facteur indispensable pour sécuriser les accès aux services cloud.
- Les pares-feux et le filtrage réseau : installation d'un firewall (pfSense, Fortigate, etc.) avec filtrage des flux entrants et sortants.
- Les mises à jour régulières : application systématique des correctifs de sécurité sur les serveurs, les postes clients et les équipements réseau.
- La sensibilisation : formation régulière des employés aux risques liés au phishing et aux bonnes pratiques afin d'améliorer la sécurité.

Exemple d'application concrète

Pour une PME de 25 salariés avec un budget limité, je proposerais :

- Un pare-feu pfSense ;
- Une sauvegarde cloud chiffrée et automatisée ;
- L'activation du MFA sur Microsoft 365 ;
- Une politique de mots de passe sécurisée ;
- Une formation annuelle à la cybersécurité ;
- Une supervision minimale des équipements.

Ces solutions permettraient d'atteindre un niveau de sécurité cohérent avec la situation financière de l'entreprise.

La cybersécurité dans les PME est un sujet central et en constante évolution. En tant que futur professionnel en SISR, cette veille me permet de rester informé, d'anticiper les risques et de proposer des solutions concrètes afin de sécuriser efficacement une infrastructure informatique.