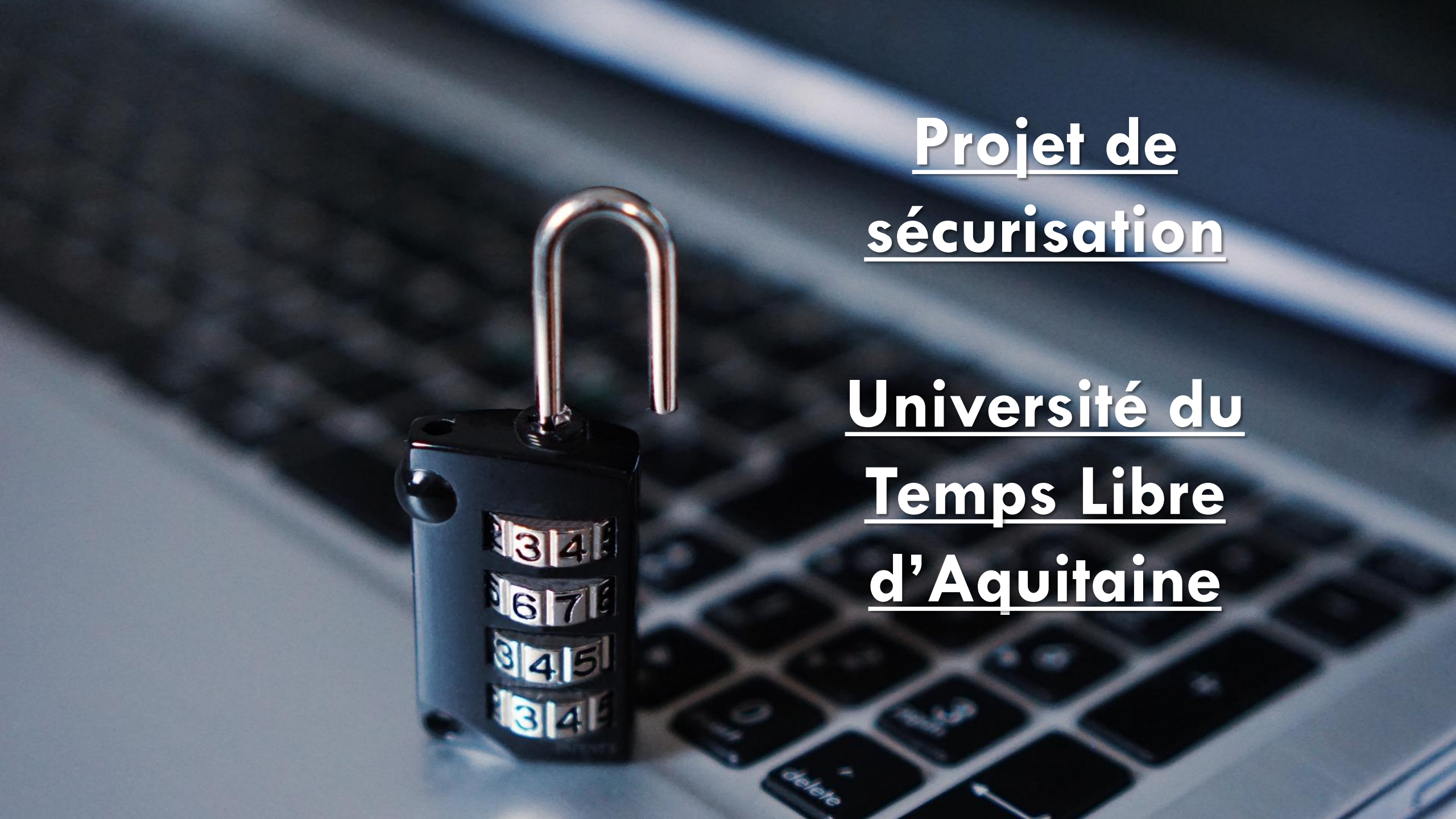

Projet de sécurisation

Université du Temps Libre d'Aquitaine

Contexte

Mise en place d'une salle informatique par une association au sein d'une université

- **Accès libre:** Gratuit, sans engagement, avec inscription préalable
- **Locaux prédéterminés:** salle de TP par l'université
- **Politique de sécurité :** normes selon les standards de sécurité
- **Périmètre:** sécurisation de la salle informatique uniquement

Expression du besoin

- Séances de 50 minutes à heure fixe
- Accès à internet, possibilité d'envoyer des mails
- Matériel qui ne dépend pas de l'association: peu de modifications possibles
- Sécuriser le mieux possible sans impacter le budget existant

Mode de fonctionnement spécifique à prendre en compte pour la mise en place des règles de sécurité

Sécurité logique

Points principaux:

Paramétrage du proxy/parefeu: paramétrage du proxy/parefeu pour l'accès par internet aux sites autorisés

Sécurisation du serveur : renforcement de la sécurité du serveur, un seul compte administrateur

Protection du réseau: installation de l'antivirus utilisé par l'université ainsi que le profil de sécurité à harmoniser sur tous les postes et le serveur. Voir s'il est possible de mettre en place des comptes temporaire pour chaque utilisateurs inscrits (complexe).

Traçabilité: Tenu du registre au moment de l'inscription: attribution d'un poste informatique pour la tranche horaire indiquée.
Conservation et analyse des logs (évènements, incidents…) de sécurité

Accès: comptes utilisateurs avec accès aux ressources limités aux besoins métiers,
accès aux ordinateurs selon la plage horaire de travail

Confidentialité: écran de mise en veille avec verrouillage

Sécurité logique

Points principaux:

Politique de BYOD: lorsque les utilisateurs récupèrent leurs travaux avec leurs clefs USB,
Il faudrait clairement indiquer aux utilisateurs que les programmes malveillants sont interdits.
Dans tous les cas, scan de l'antivirus au niveau des ports USB,

Prise en main à distance: l'animateur aura la possibilité d'utiliser un logiciel de prise en main à distance non intrusif et qui nécessitera de demander l'autorisation à l'utilisateur client (VNC, remote desktop manager…)

Règles du réseau: connexion des postes au réseau selon des règles du type GPO afin de mettre à jour régulièrement les logiciels et les systèmes d'exploitation, permettre de remettre la configuration Initiale des postes entre chaque séances.

Imprimante: Désactiver le wi-fi (usage ethernet) , enregistrement des logs d'impressions et configuration des paramètres de sécurité de l'imprimante.

Confidentialité: écran de mise en veille avec verrouillage, usage des logiciels libres bureautique et mails (thunderbird ?) conformes à la charte informatique

Sécurité physique et accès

Points principaux:

Antivols: câbles de sécurité à disposer sur les 10 unités centrales + écrans et le serveur (activer la serrure de sécurité et la protection antivol)

Incendie: vérification régulière du détecteur de fumée et des extincteurs, contrôler L'alimentation électrique de la baie de brassage et des locaux régulièrement

Continuité des activités: Si il y a des générateurs de secours déjà présent dans l'immeuble, utiliser également des sondes pour le local

Accès aux locaux: s'assurer que la gestion de l'accès au local est règlementé surtout en dehors des horaires autorisés

Périphériques: ranger les consommables et matériels dans l'armoire avec inventaire régulier. Les clefs en double seront attribués aux personnes habilités à ouvrir cette armoire.

Traitement des données

Points principaux:

Politique de sécurité: s'aligner avec les règles de sécurité définies par l'université avec usage limité des données personnelles. Préciser à l'utilisateur que l'enregistrement des logs sera effectué et qu'une prise en main à distance est possible en cas de problème,

Charte informatique: signature de la charte informatique par les utilisateurs et des conditions d'acceptation concernant la récolte et le traitement des données personnels

Conformité: traitement des données conformément au RGPD (consentement avisé, délais de conservation, mesures de signalement en cas d'attaques…)

Sensibilisation: expliquer (rapidement en début de session) les risques liés aux tentatives de social engineering, adopter une démarche prudente lors de l'usage des ressources informatiques (internet, mail)

Sauvegardes: automatiser et planifier les sauvegardes des données chaque semaine

Planning

Mise en place des règles: 2 journées

Personnel: 2 techniciens, 1 administrateur

Formation du personnel : -

Matériel: 10 cadenas et câbles, 1 sonde

Réunion de mise en place: 1 journée

Conclusion de la proposition

- Des mesures de sécurité alignées avec la politique de sécurité
- **Faible coûts** et rapidité de la mise en place
- **Forte réduction des risques** après la mise en place des contrôles
- Répond à l'expression du besoin sans gêner les utilisateurs